UNIVERSIDAD NACIONAL DE INGENIERÍA

Recinto Universitario "Simón Bolívar"

Facultad de Electrotecnia y Computación

TRABAJO MONOGRAFICO

Plan de Auditoria de Sistemas de Información de la Seguridad Física en la División de Tecnologías de la Información y Comunicación DTIC-UNI

Elaborado por:

Br. Jean François Valencia **No. Carnet: 2009-29588**

Carrera:

Ingeniería en Computación

Tutor:

Msc. Jorge J. Prado Delgadillo

Managua, Nicaragua

Octubre, 2018

DEDICATORIA.

De manera muy especial dedico este logro a Dios por haberme dado la oportunidad de prepararme académicamente a nivel universitario, brindándome salud y sobre todo por haber respaldado todos mis planes y metas. A mi madre Yadira Azucena Valencia Mendoza por todo el apoyo, los sacrificios, el amor y confianza depositados en mi persona. También al resto de mi familia por su aprecio, respeto y apoyo, así como a mis compañeros de estudios y docentes que en determinado momento me apoyaron durante mi proceso de formación.

AGRADECIMIENTOS.

Por haberme apoyado en la realización de este trabajo tan importante para mí, ¡Gracias!

Msc. Ing. Jorge Prado D.
Tutor

A la División de Tecnologías de la Información y Comunicación DTIC- UNI, por brindarme el espacio para la realización de esta auditoría y a todo el equipo de docentes de la Facultad de Electrotecnia y Computación por haberme ayudado en mi formación académica.

CONTENIDO

I. INTRODUCCIÓN

El presente documento detalla un plan de Auditoria de Sistemas de Información de la Seguridad Física a la División de Tecnologías de la Información y Comunicación (DTIC), instancia que depende de la rectoría de la Universidad Nacional de Ingeniería y la cual, asesora, planifica, supervisa y ejecuta proyectos institucionales de Tecnologías de Información, brinda servicios tecnológicos a la comunidad universitaria, para agilizar y facilitar los procesos de las actividades académicas y administrativas; enmarcados en políticas y estándares internacionales establecidos y adaptados a la realidad institucional y nacional.

Esta división como parte de su crecimiento hace uso de las TIC´s para sistematizar los procesos en las distintas áreas administrativas y académicas de la Universidad procurando ofrecer un servicio de calidad a los usuarios de la UNI.

La DTIC, se compone principalmente en 3 áreas: área de Infraestructura de Redes y Soporte técnico, área de Administración de Servidores y área de Sistemas de Información.

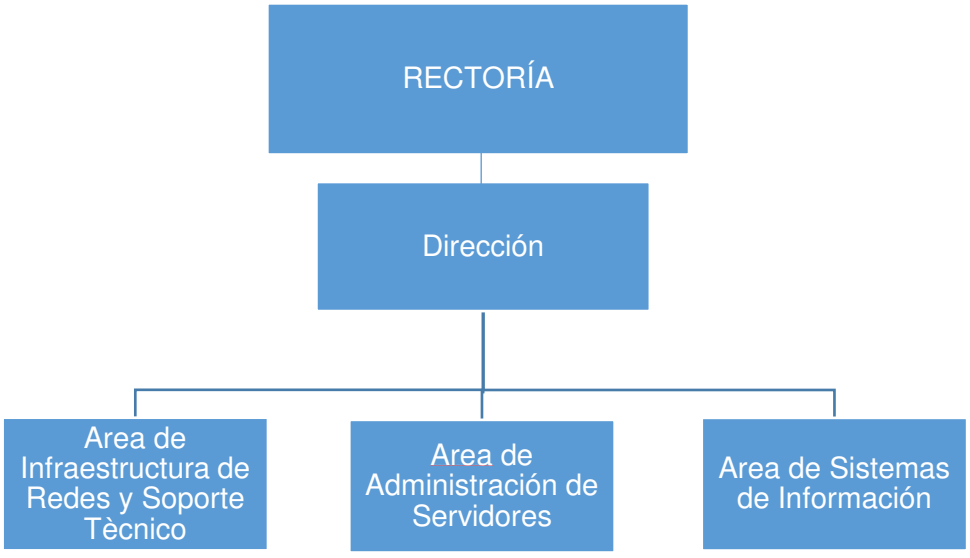

Fig.1 Estructura de la DTIC.

El área de Infraestructura de Redes y Soporte Técnico es la encargada de:

- Atención de contingencias informáticas en datos y aplicaciones de cómputo.
- Análisis y recuperación de datos e información en ambiente Windows.
- Instalación, configuración y mantenimiento de sistemas operativos y paquetería de cómputo.
- Evaluación y diagnóstico de aplicaciones y equipos de cómputo y de redes de computadoras.

La principal función del área de Infraestructura de Redes y Soporte Técnico es la administración tecnológica de las redes de computadoras, manteniendo funcionando efectivamente los servidores, switches, equipos inalámbricos, computadoras de escritorio, así como laptops que presenten fallas para poder conectarse a Internet o presenten algún otro incidente por el cual el usuario no logre ejercer su trabajo eficientemente.

El área de Administración de Servidores se encarga de servicios como:

- Alojamiento WEB
- Correo Institucional

El área de Sistemas de Información se encarga de atención de incidencias en los siguientes sistemas informáticos:

- SIRA (Sistema de Registro Académico)
- Notas en Línea
- Registro de Calificaciones
- SIPPSI (Sistema de Información de Planificación, Presupuesto y Seguimiento Institucional)
- SISPRE (Sistema de Presupuesto)
- SIFOP (Sistemas de Facultades o Programas)
- SIAF (Sistema de Inventario)

- SAF (Sistema de Activo Fijo)
- SISEP (Sistema de Ejecución Presupuestaria)
- MIC-SIFOP (Sistema de Ingresos y Egresos por Estructura Programática)
- SIRRHH (Sistema de Recursos Humanos)
- SISCOM (Sistema de Compras)
- SIPAD (Sistema de Procesos Administrativos)
- Soporte y mantenimiento en los diferentes sistemas de información utilizados en la institución.
- Implementación de controles y mecanismo de seguridad en el acceso de los sistemas de información.
- Efectuar respaldos periódicos de las bases de datos generadas por los sistemas de información institucional.
- Brindar capacitación sistemática a los usuarios de la institución en el manejo de los sistemas de información institucional.

II. ANTECEDENTES

La División de Tecnologías de la Información y Comunicación DTIC, carece de antecedentes previos de Auditoria de Sistemas de Información de la Seguridad Física, así como también de documentación similar a una buena gestión de la seguridad física, su gestión consiste en la utilización de un sistema de mesa de ayuda (helpdesk), donde registran todas las incidencias del área de Infraestructura de Redes y Soporte Técnico, como también, del área de Administración de Servidores para realizar un seguimiento y control de las incidencias atendidas a los usuarios de la UNI, gestión que no contempla la seguridad física de la división, es por ello que nace esta propuesta de Auditoria de Sistemas de Información de la Seguridad Física como parte de la innovación en cuanto al tema y marcar un antecedente del mismo, además de ser un tema de interés tecnológico que contribuirá a la gestión de buenas prácticas de seguridad física en la DTIC y en la cual aplicaré mis conocimientos adquiridos durante los años de estudio en la carrera de Ingeniería en Computación.

El Centro de Datos de la UNI ubicado desde un inicio en el edificio de la Facultad de Electrotecnia y Computación (FEC), 2da planta, es administrado por la DTIC desde el año 2006 y nace con financiamiento de la cooperación internacional (Agencia Sueca para el desarrollo Internacional ASDI).

Actualmente, con la aprobación de un proyecto de nueva ubicación e instalación del Centro de Datos de la UNI se pretende modernizar los equipos de redes y su infraestructura para brindar un mejor servicio de ancho de banda de Internet a todas las áreas administrativas y académicas de la Universidad. Ubicado estratégicamente en el sótano del edificio Rigoberto López Pérez, se realizaron todos los estudios correspondientes en el año 2014, para ser aprobado por la dirección superior del consejo Universitario en el año 2015 solicitando la partida presupuestaria a través de un préstamo que realizo la Universidad en el año 2016, para finalmente implementarse en el mes de mayo de 2017 y ser administrado actualmente por el área Nic.ni la cual es un área de la Universidad Nacional de Ingeniería (UNI) que además de administrar los dominios **NIC.NI** a nivel mundial,

ofrece servicios de hosting, página web y otros, que son de mucha utilidad para los jóvenes universitarios, la sociedad y el país.

En las nuevas instalaciones del Centro de Datos de la UNI, es donde se aplicará el Plan de Auditoria de Sistemas de Información de la Seguridad Física utilizando la metodología COBIT 4.1 para determinar si estas instalaciones son las adecuadas en términos de seguridad física para una buena gestión de tecnologías de la información.

III. JUSTIFICACION

Descripción del problema

En el área de la DTIC, carece de un control de sistematización de procesos y procedimientos adecuados para la seguridad física y del entorno, cuenta con poca o inexistentes seguridades de los recursos informáticos y humanos de la División debido a que no existen políticas internas bien definidas, y a estas circunstancias se les suma:

1. Falta parcial de seguridades lógicas y físicas que garanticen la seguridad de equipos informáticos e información.

2. Carece de documentación para los procedimientos de la seguridad física.

3. Existe la necesidad de implementar procesos de gestión del entorno físico que garanticen la integridad y seguridad del personal.

IV. OBJETIVOS

Objetivo General

Desarrollar un Plan de Auditoria Informática de la Seguridad Física en la División de Tecnologías de la Información y Comunicación DTIC UNI-RUBS

Objetivos Específicos

- Evaluar la situación actual de la DTIC en cuanto a seguridad física basado en la normativa COBIT 4.1.

- Identificar vulnerabilidades de seguridad física en los recursos, (tecnología, instalaciones, personal, comunicaciones de redes).

- Aplicar técnicas de auditoria informática de la seguridad física como análisis de la información recabada, entrevista, cuestionarios e informe para la evaluación de controles enfocados en los riesgos de seguridad física.

- Presentar informe de hallazgos y recomendaciones obtenidos de la ejecución del plan de auditoria.

V. MARCO TEÓRICO

Para esta auditoria se implementó los Objetivos de Control para Tecnologías de Información y Tecnología Relacionada (COBIT), elaborado por el IT Governance Institute, bajo el auspicio de ISACA, Information Systems Audit and Control Association. Esta herramienta de auditoria permitió elaborar una auditoria de la seguridad física con todos los estándares internacionales con el propósito de evaluar los controles de seguridad física que se utilizan actualmente en la DTIC.

COBIT es un conjunto de objetivos de control aplicables a un ambiente de tecnología de información que lograron definirse gracias a un trabajo de investigación en búsqueda de mejores conductas, prácticas y requerimientos de la industria, el cual combina los principios contenidos por modelos existentes y conocidos, como COSO, SAC y SAS.

COSO: "*La misión del Comité de Organizaciones Patrocinadoras (COSO) es proporcionar liderazgo reflexivo mediante el desarrollo de marcos integrales y orientación sobre gestión de riesgos empresariales, control interno y disuasión del fraude diseñados para mejorar el desempeño y la gobernanza organizacional y reducir el alcance del fraude en las organizaciones*"[1]

SAC: Una herramienta integral que brinda orientación sobre auditoría interna y auditoría de sistemas de información. Fue el primer marco de control interno que se enfocó en la tecnología de la información. SAC fue publicado originalmente por el Instituto de Auditores Internos en 1977, con una actualización significativa en 1991 y una revisión posterior en 1994. Fuente: Champlain, sistemas de información de auditoría: 2003

SAS: Las Declaraciones de Normas de Auditoría o SAS (Statements on Auditing Standards) son interpretaciones de las normas de auditoría generalmente aceptadas que tienen obligatoriedad para los socios del American Institute of

1 www.coso.org. (29 de enero de 2018). https://www.coso.org/Pages/aboutus.aspx

Certified Public Accountants AICPA, pero se han convertido en estándar internacional, especialmente en nuestro continente. Las Declaraciones de Normas de Auditoría son emitidas por la Junta de Normas de Auditoría (Auditing Standard Board ASB).

La misión de COBIT es Investigar, desarrollar, publicar y promover un conjunto de objetivos de control para tecnología de información, que sea internacional y este actualizado para uso cotidiano de gerentes, auditores y usuarios, obteniendo como ventajas:

-Mejores prácticas en calidad y seguridad.

-Tomas de decisiones.

-Uso de indicadores de medición.

Usuarios:

- **La gerencia:** para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- **Los usuarios finales:** quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- **Los auditores:** para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
- **Los responsables de TI:** para identificar los controles que requieren en sus áreas.

También puede ser utilizado dentro de las empresas por el responsable de TI en su responsabilidad de controlar los aspectos de información y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

Características:

- Orientado al negocio.
- Alineado con estándares y regulaciones.
- Basado en una revisión crítica y analítica de las tareas y actividades en TI alineado con estándares de control de auditoria (COSO, IFAC, IIA, ISACA, AICPA).

5.1 Marco de Trabajo de COBIT

Los recursos de TI son manejados por procesos para lograr metas de TI que respondan a los requerimientos del negocio.

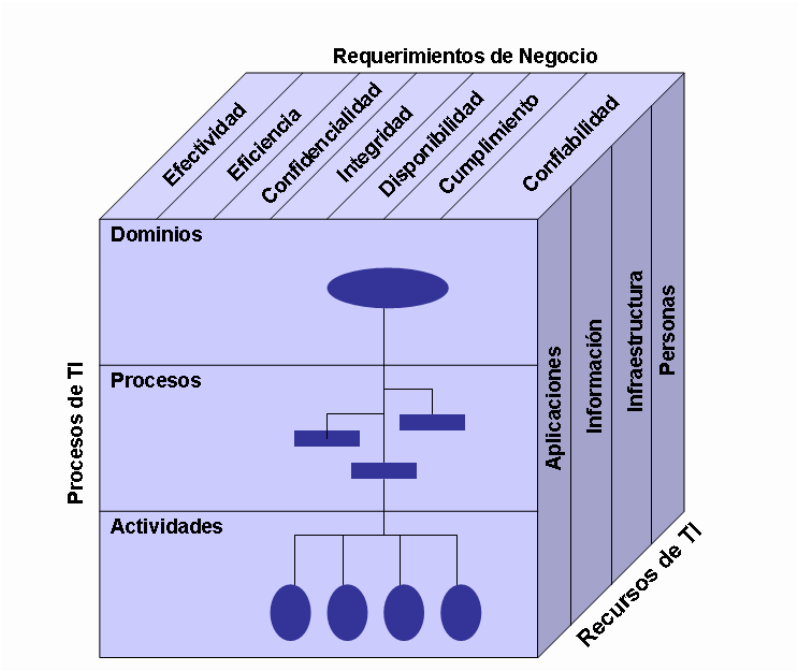

Fig.2 Principio básico del marco de trabajo COBIT.

5.2 Concepto de Auditoria

Actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Sus principales características son:

- **Contenido:** una opinión
- **Condición:** profesional
- **Justificación:** sustentada en determinados procedimientos (la opción profesional se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma).
- **Objeto:** una determinada información obtenida en un cierto soporte.
- **Finalidad:** determinar si se presenta adecuadamente la realidad o esta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

Siempre es un proceso que se realiza a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión. (Ruiz, 2000, págs. 3-5)

5.3 Auditoria de Sistemas de Información

Es más correcto y más genérico hablar de Auditoria de Sistemas de Información (ASI) que de Auditoria Informática. El primer término engloba al segundo y también a los procesos y medios no automáticos que forman parte del sistema de información de una organización:

Auditoria: Herramientas y métodos para establecer criterios que permitan medir la eficacia, eficiencia y conformidad con los objetivos deseados de un determinado sistema

Sistemas de información: eficacia, eficiencia y conformidad con los objetivos del sistema de información.

5.4 Objetivos fundamentales de ASI:

- **De protección de los Activos y Recursos:** Verificar que existe un sistema de control interno que protege los activos materiales e inmateriales de la instalación informática de cualquier posible amenaza o riesgo.

- **De Integridad de Datos:** El sistema de control interno debe tener mecanismos que vigilen constantemente el mantenimiento de la integridad de los datos.

- **De Efectividad del Sistema:** Un sistema de información efectivo alcanza sus objetivos. Estos objetivos dependen de las características y necesidades de los usuarios y de los canales y procedimientos de decisión.

- **De Eficiencia del Sistema:** Un sistema de información eficiente utiliza el mínimo de recursos necesarios para obtener las salidas requeridas. La eficiencia no debe medirse de forma aislada sino considerando el conjunto de procesos y los recursos disponibles.

5.5 Principales tipos de ASI:

De la **Organización** y **Gestión del Departamento de Informática:** Políticas, estructuras de gestión y organizativas, procedimientos operativos y entorno de control.

De la **Seguridad Física y Lógica**: Políticas, procedimientos y planes para proteger la información y el sistema de información.

De las **Tecnologías de la Información:**

- De los computadores
- De bases de datos
- De proceso de datos distribuido y control de datos en red
- De redes locales
- Del desarrollo de un proyecto
- De intercambio electrónico de datos

- De herramientas (CASE, etc.)

5.6 Auditoria Física

La auditoría física es el medio que va a proporcionar la evidencia o no de la seguridad física en el ámbito en el que se va a desarrollar la labor profesional. Es por tanto necesario asumir que la auditoria física no se va a limitar a comprobar la existencia de los medios físicos, sino también su funcionalidad, racionalidad y seguridad. Garantiza la integridad de los activos humanos, lógicos y materiales de un centro de procesamientos de datos.

5.7 Criterios de Información

Para satisfacer los objetivos de la división, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Para esto se definieron los siguientes criterios de información:

- Requerimientos de **Calidad:**
- Calidad
- Coste
- Entrega (servicio)

- Requerimientos **Fiduciarios:**
- Efectividad y eficiencia de las operaciones
- Fiabilidad de la información
- Cumplimiento de las leyes y normas

- Requerimientos de **Seguridad:**
- Confidencialidad
- Integridad
- Disponibilidad

5.8 Recursos de TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio.

En COBIT se establecen los siguientes **recursos en TI** necesarios para alcanzar los objetivos de negocio:

- **Datos:** Todos los objetos de información. Considera información interna y externa, estructurada o no, graficas, sonidos, etc.

- **Aplicaciones:** Entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.

- **Tecnología:** Incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

- **Instalaciones:** Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

- **Recurso Humano:** Por habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de información.

5.9 Procesos de TI

La estructura de COBIT se define a partir de una premisa simple y pragmática: "los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que

proporcionen la información que la empresa necesita para alcanzar sus objetivos".

COBIT se divide en tres niveles:

1. **Dominios:** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
2. **Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control.
3. **Actividades:** Acciones requeridas para lograr un resultado medible.

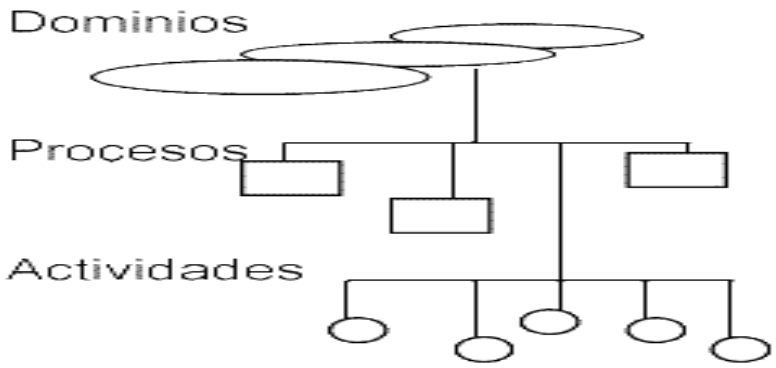

Fig.3 Procesos de TI.

Se definen 34 objetivos de control generales, uno para cada uno de los procesos de TI. Estos procesos están agrupados en cuatro grandes dominios:

-Planificación y organización

-Adquisición e implementación

-Suministro y Soporte

-Supervisión

El dominio de entrega de servicio y soporte de la versión 4 de COBIT, contempla los aspectos relativos a la gestión de la seguridad y la continuidad de las operaciones e incluye un objetivo de control de alto nivel específico para la seguridad física y del entorno. Este objetivo de control hace hincapié en que para una adecuada protección de las personas y de los elementos que componen un sistema de información son necesarias unas instalaciones bien diseñadas y bien gestionadas. [2]

Los procesos de gestión del entorno físico deben incluir la definición de los requisitos que deben cumplir los edificios y localizaciones donde vayan a residir los elementos de nuestro sistema de información, la selección de locales e instalaciones, así como el diseño de los procesos necesarios para supervisar los factores ambientales y gestionar el acceso físico a las instalaciones y recursos. Una gestión adecuada y efectiva del entorno reduce la frecuencia de las interrupciones del funcionamiento habitual del negocio, ocasionadas por daños a los equipos y al personal.

Según COBIT, el objetivo de control de alto nivel DS 12 Gestión de Entorno Físico es un control sobre el proceso de TI (Tecnologías de la información), que satisface el requisito de negocio de TI, proteger los activos de TI y la información del negocio, minimizando el riesgo de una interrupción del servicio.

Este objetivo de control está dirigido a proporcionar y mantener un entorno físico adecuado para proteger los activos de TI contra acceso, daño o robo. Para ello es necesario implementar medidas de seguridad física, así como seleccionar y gestionar las instalaciones donde residen los elementos del sistema de información.

Así mismo, es necesario medir su efectividad, para ello se utilizan los siguientes indicadores:

2.- (Piattini Velthuis & del Peso Navarro, 2008, pág. 289)

- Tiempo sin servicio ocasionado por incidentes relacionados con el entorno físico.
- Número de incidentes ocasionados por fallos o vulnerabilidades de seguridad física.
- Frecuencia de la revisión y evaluación de los riesgos físicos.

5.10 DS12-Administracion del Ambiente Físico

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

La administración del ambiente físico se descompone en los cinco objetivos de control detallados que se describen a continuación:

DS12.1-Selección y diseño del centro de procesos de datos.

DS12.2-Medidas de seguridad física.

DS12.3-Acceso físico.

DS12.4-Protección contra factores ambientales.

DS12.5-Gestion de las instalaciones.

5.10.1 Selección y diseño del centro de procesos de datos:

Esta selección debe realizarse teniendo en cuenta los riesgos asociados a los desastres naturales como a los provocados por el hombre, también se debe considerar la legislación aplicable como las leyes y los reglamentos relativos a la seguridad y la salud en el trabajo.

5.10.2 Medidas de seguridad física:

Se deben definir e implementar las medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al establecimiento de un perímetro de seguridad, de zonas de seguridad, la ubicación de los equipos críticos y de las zonas de carga y descarga. Deben definirse las responsabilidades relativas a los procedimientos de supervisión, informe y resolución de los incidentes de seguridad física.

5.10.3 Acceso físico:

Se deben definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo los accesos en caso de emergencia. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y supervisarse. Esto es aplicable a todas las personas que accedan a las instalaciones, incluyendo personal propio, clientes, proveedores, visitantes o cualquier otra persona.

5.10.4 Protección contra factores ambientales:

Se deben diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipos adecuados para la supervisión y control del entorno.

5.10.5 Gestión de las instalaciones:

Se deben gestionar las instalaciones, incluyendo los equipos de comunicaciones y suministro de energía, de acuerdo con las leyes y los reglamentos aplicables, los requerimientos técnicos y del negocio, las especificaciones de los proveedores y los requisitos relativos a la seguridad y a la salud en el trabajo.

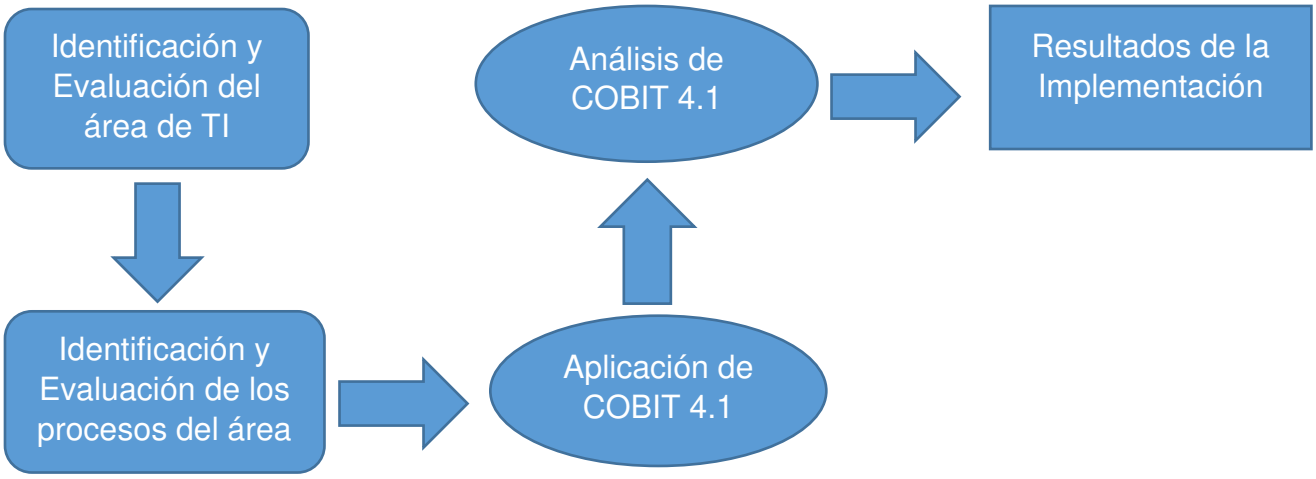

Fig.4 Fases de auditoria.

	ENLACE DE LAS METAS DE TI A PROCESOS DE TI																		
													Criterios de información						
	Metas de TI	Procesos											Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
1	Responder a requerimientos de negocio alineado con la estrategia de negocio	P01	P02	P04	P010	AI1	AI6	AI7	DS1	DS3	ME1	P	P		S	S		
2	Responder a los requerimientos de gobierno en línea con la dirección ejecutiva	P01	P04	P010	ME1	ME4						P	P					
3	Asegurar la satisfacción del usuario final con la oferta de servicios y niveles de servicio	P08	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P		S	S		
4	Optimizar el uso de la información	P02	DS11										S		P			S
5	Crear agilidad de TI	P02	P04	P07	AI3							P	P		S			
6	Definir como la funcionalidad de negocio y requerimientos de control se trasladan en soluciones efectivas	AI1	AI2	AI6								P	P				S	
7	Adquirir y mantener sistemas de aplicación integrados y estandarizados	P03	AI2	AI6								P	P				S	
8	Adquirir y mantener una infraestructura de TI integrada y estandarizada	AI3	AI5									S	P					
9	Adquirir y mantener habilidades de TI que responden a la estrategia de TI	P07	AI5									S	P					
10	Asegurar la satisfacción mutua de relaciones con terceras partes	DS2										P	P	S	S	S	S	S
11	Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos del negocio	P02	AI4	AI7								P	P		S	S		
12	Asegurar la transparencia y comprensión de costes de TI, beneficios, estrategia, políticas y niveles de servicio	P05	P06	DS1	DS2	DS6	ME1	ME4				P	P				S	S
13	Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnología	P06	AI4	AI7	DS7	DS8						P	S					
14	Tener en cuenta y proteger todos los activos de TI	P09	DS5	DS9	DS12	ME2						S	S	P	P	P	S	S
15	Optimizar la infraestructura, recursos y capacidades de TI.	P03	AI3	DS3	DS7	DS9						S	P					
16	Reducir los defectos de la solución y entrega de servicio y reelaborar	P08	AI4	AI6	AI7	DS10						P	P		S	S		
17	Proteger el logro de los objetivos de TI	P09	DS10	ME2								P	P	S	S	S	S	S
18	Establecer la claridad del impacto de negocio de los riesgos a los objetivos y recursos de TI	P09										S	S	P	P	P	S	S
19	Asegurar que la información crítica y confidencial se retiene a aquellos que no deben tener acceso	P06	DS5	DS11	DS12									P	P	S	S	S
20	Asegurar que las transacciones de negocio automatizadas y los cambios a la información son confiables	P06	AI7	DS5								P			P	S	S	
21	Asegurar que los servicios de TI y la infraestructura pueden resistir apropiadamente y recuperar fallos debido a errores, ataques deliberados o desastres	P06	AI7	DS4	DS5	DS12	DS13	ME2				P	S		S	P		
22	Asegurar el mínimo impacto de negocio en caso de una interrupción de servicios de TI o cambios	P06	AI6	DS4	DS12							P	S		S	P		
23	Estar seguros que los servicios de TI están disponibles según se requiere	DS3	DS4	DS8	DS13							S	P					
24	Mejorar la eficiencia de costes de TI y sus contribuciones a la rentabilidad del negocio	P05	DS6									S	P					S
25	Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estandares de calidad	P08	P010									P	P		S			S
26	Mantener la integridad de la información e infraestructura de procesamiento	AI6	DS5									P	P		P	P		S
27	Asegurar que TI cumple con la legislación, regulación y contratos.	DS11	ME2	ME3	ME4									S	S		P	S
28	Asegurar que TI demuestra la eficiencia de costes de la calidad de servicios, mejoras continuas y disposición para cambios futuros.	P05	DS6	ME1	ME4							P	P					P

Fig.5 Enlace de metas de TI a Procesos de TI

5.11 Conocer los procesos de TI

En esta etapa se obtiene cada uno de los procesos del área de TI, junto con su documentación. Con el fin de determinar que está establecido como proceso y la forma en que se documenta. En esta documentación se incluirán los siguientes ítems:

- Nombre del proceso
- Descripción del proceso
- Objetivo
- Actividades: Que actividades apoyan la ejecución del proceso, la descripción de cada una de estas y además quienes son los responsables de las mismas.
- Métricas: Como se está midiendo la correcta ejecución del proceso o la efectividad del mismo.
- Procesos relacionados: Que otros procesos están relacionados con el proceso.
- Responsable(s).
- Importancia o criticidad: Que importancia o criticidad tiene el proceso para el área de TI.

5.12 Plantilla de Procesos

PLANTILLA DE PROCESOS	
Nombre del Proceso	Administrar el ambiente Físico
Descripción	La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

<table>
<tr><td>Objetivos</td><td>-Selección y Diseño del Centro de Datos
-Medidas de Seguridad Física
-Acceso Físico
-Protección contra Factores Ambientales
-Administración de Instalaciones Físicas</td></tr>
<tr><td>Métricas (Como se está midiendo la correcta ejecución del proceso o la efectividad del mismo)</td><td>✓ Tiempo sin servicio ocasionado por incidentes del ambiente físico.
✓ Numero de lesiones causadas por el ambiente físico.
✓ Riesgos de seguridad causados por incidentes de seguridad física.
✓ Número de incidentes causados por fallas o violaciones a la seguridad física.
✓ Número de incidentes causados por acceso no autorizado a las instalaciones de cómputo.
✓ Frecuencia de entrenamiento del personal respecto a medidas de protección, seguridad y de instalaciones.
✓ Porcentaje de personal entrenado en medidas de protección, seguridad y de instalaciones.
✓ Número de pruebas de mitigación de riesgos realizadas en el último año.
✓ Frecuencia de las revisiones y evaluaciones de riesgo físico.</td></tr>
<tr><td>Procesos Relacionados (Que otros procesos están relacionados con el proceso)</td><td>
<table>
<tr><th>DESDE</th><th>ENTRADAS</th><th>SALIDAS</th><th>HACIA</th></tr>
<tr><td>PO2</td><td>Clasificaciones asignadas a los datos</td><td rowspan="3">Reportes de desempeño de los procesos</td><td rowspan="3">ME1</td></tr>
<tr><td>PO9</td><td>Evaluación de riesgo</td></tr>
<tr><td>AI3</td><td>Requerimientos del ambiente físico</td></tr>
</table>
</td></tr>
</table>

Responsables	Mgp.Sixto Chavarría Director Ejecutivo Ing. Carlos Rodríguez Responsable del área de Infraestructura de Redes y Soporte Técnico Ing. Walter Pérez Responsable del área de Administración de Servidores Ing. Luis Pérez Responsable del área de Sistemas de Información

En cuanto a los procesos relacionados **PO2. Definir la Arquitectura de la información** recomienda:

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias de la división. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de información compartida a lo largo de las aplicaciones y de las entidades.

Que satisface el requerimiento del negocio de TI para:

Agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos del negocio.

Enfocándose en

El establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos.

Se logra con

- ✓ El aseguramiento de la exactitud de la arquitectura de la información y del modelo de datos.
- ✓ La asignación de propiedad de datos.
- ✓ La clasificación de la información usando un esquema de clasificación acordado.

Se mide con

- ✓ El porcentaje de elementos de datos redundantes/duplicados.
- ✓ El porcentaje de aplicaciones que no cumplen con la metodología de arquitectura de la información usada por la división.
- ✓ La frecuencia de actividades de validación de datos.

Siendo este objetivo de control **Clasificaciones asignadas a los datos** el objetivo principal relacionado con el proceso **DS12 Gestión del entorno Físico** se requiere:

Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, publica, confidencial, secreta) de la DTIC. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección y una breve descripción de los requerimientos de retención y destrucción de datos, además de que tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado.

En cuanto a los procesos relacionados **PO9. Evaluar y Administrar los Riesgos de TI** recomienda:

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los interesados y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.

Que satisface el requerimiento del negocio de TI para:

Analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio.

Enfocándose en

La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.

Se logra con

La garantía de que la administración de riesgos está incluida completamente en los procesos administrativos, tanto interna como externamente, y se aplica de forma consistente.

- ✓ La realización de evaluaciones de riesgo.
- ✓ La recomendación y comunicación de planes de acción para remediar riesgos.

Se mide con

- ✓ Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos.

- ✓ Porcentaje de riesgos críticos de TI identificados con planes de acción elaborados.
- ✓ Porcentaje de planes de acción de administración de riesgos aprobados para su implementación.

Siendo este objetivo de control **Evaluación de Riesgos de TI** el objetivo principal relacionado con el proceso **DS12 Gestión del entorno Físico** se requiere:

Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

En cuanto a los procesos relacionados **AI3 Adquirir y Mantener Infraestructura Tecnológica** recomienda:

Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convencidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

Que satisface el requerimiento del negocio de TI para:

Adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI.

Enfocándose en

Proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.

Se logra con

- ✓ El establecimiento de un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica.
- ✓ La planeación de mantenimiento de la infraestructura.
- ✓ La implantación de medidas de control interno, seguridad y auditable.

Se mide con

- ✓ El porcentaje de plataformas que no se alinean con la arquitectura de TI definida y los estándares de tecnología.
- ✓ El número de procesos de negocio críticos soportados por infraestructura obsoleta (o que pronto lo será).
- ✓ El número de componentes de infraestructura que ya no se pueden soportar (o que ya no se podrán en el futuro cercano).

Siendo este objetivo de control **Mantenimiento de la Infraestructura** el objetivo principal relacionado con el proceso **DS12 Gestión del entorno Físico** se requiere:

Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

VI. HALLAZGOS

A continuación, los principales hallazgos de mayor relevancia que se encontraron en la DTIC según la normativa COBIT 4.1:

- El centro de datos no cuenta con un servicio de habilitación municipal y de bomberos vigente.

- No se encuentran habilitadas cámaras de seguridad dentro y fuera del centro de datos.

- El personal de limpieza, mantenimiento y vigilancia no se les ha orientado sobre cómo hacer su tarea sin afectar los equipos, todo ello mediante una hoja de instrucciones escrita.

- No está trabada la carcasa del servidor de archivos o protegido de modo que no se retiren plaquetas, chips u otros dispositivos.

- El centro de datos no se encuentra en un piso intermedio.

- No existe una bóveda externa en la que se guarde las copias de respaldo y que cuente con adecuadas medidas de seguridad física que incluyen protección contra fuego, contra robos y adecuados controles de temperatura y humedad.

- No existe un estudio específico de riesgo de incendio, considerando los aspectos protección y prevención, con un seguimiento de las recomendaciones prescritas.

- No existen extinguidores manuales en la sala de cómputos.

- Los cables eléctricos empotrados y en cañerías no tienen un adecuado sistema de resistencia al fuego.

- No existen detectores de agua debajo de pisos sobre elevados y cerca de los drenajes del piso que se activen mediante señal audible.

- No existen detectores de agua ubicados encima de cielorrasos.

- No se determina en que zonas del Centro de Cómputos debe prohibirse el fumar, señalizándolas mediante carteles y no se vigila el cumplimiento

estricto de esta medida.

- En algunas áreas, como centros de cómputo los switches, hubs y routers están a simple vista y eventualmente de fácil acceso o manipulación para el usuario.

- Los medios de control de acceso físico no son coherentes con las eventuales necesidades de evacuación de personas en caso de desastre y no se desactiva automáticamente en caso de alarma.

- No existe un dispositivo alternativo para evacuar al personal de la sala de operaciones en caso de desastre que inhabilite los sistemas normales de ingreso y egreso.

- Al adquirir equipamiento de oficina para el Centro de Cómputos, no se evalúa su resistencia al fuego.

- No existen dentro del Centro de Cómputos muebles ignífugos donde guardar material sensible.

- No ha sido probado el grupo electrógeno dentro del último semestre.

Introducción al Modelo de Madurez

Los modelos de madurez facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad.

En el área de TI el dueño del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control. Esto responde a tres necesidades:

1. Una medición relativa de donde se encuentra la empresa.
2. Una manera de decidir hacia donde ir de forma eficiente.
3. Una herramienta para medir el avance contra la meta.

El modelo de madurez para la administración y el control de procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a si misma desde un nivel de no-existente (0) hasta un nivel optimizado (5). Este enfoque se deriva del modelo de madurez que el software engineering instituto definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar donde se encuentran los problemas y como fijar prioridades para las mejoras. El propósito no es evaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Con los modelos de madurez de COBIT, a diferencia de la aproximación del CMM original de SEI, no hay intención de medir los niveles de forma precisa o probar a certificar que un nivel se ha conseguido con exactitud.

Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales, donde se presentaran como un medio para dar soporte al caso de

negocio para planes futuros, se requiere contar con un buen método grafico de presentación:

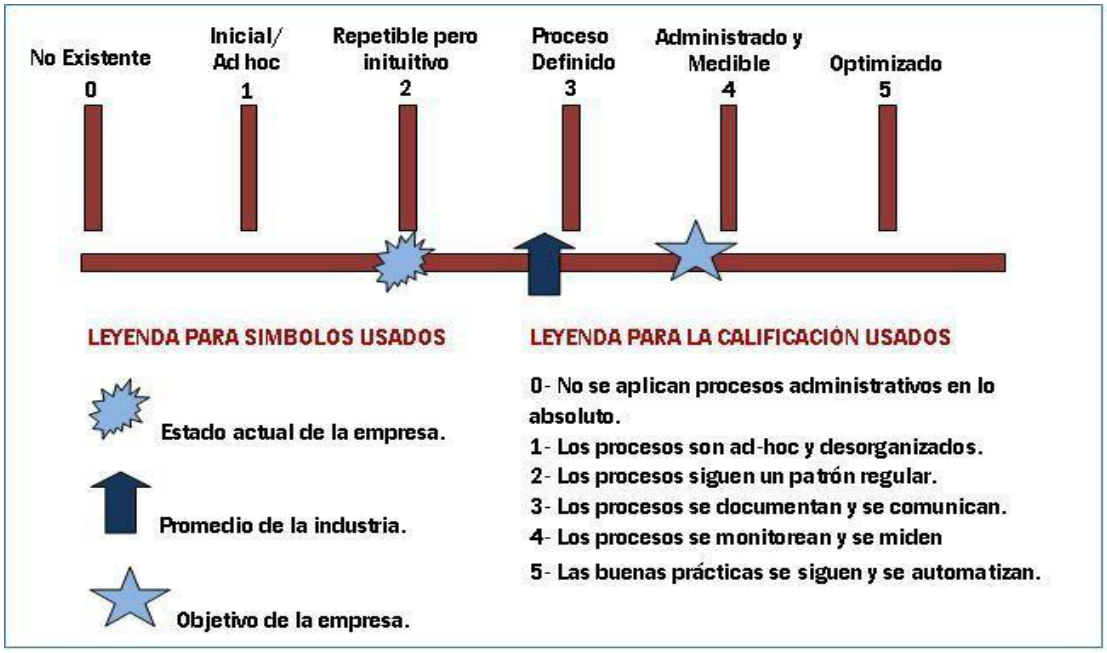

Fig.6 Ejemplo de grafica de nivel de madurez.

El desarrollo se basó en las descripciones del modelo de madurez genérico descritas en la tabla siguiente:

MODELO GENERICO DE MADUREZ	
0 No Existente	No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de computo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.

1 Inicial	La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.
2 Repetible	Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.
3 Definido	Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de computo controlado. los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de computo solo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.
4 Administrado	Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance de trabajo, servicios/entregables a suministrar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades para la administración del contrato del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas.
	Hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente computo de la organización. Los estándares están

5 Optimizado	definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales (por ejemplo: fuego, rayos, inundaciones, etc.). Se clasifican y se hacen inventarios de todas las instalaciones de acuerdo con el proceso continuo de administración de riesgos de la organización. El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. El ambiente se monitorea y controla por medio de equipo especializado y la salas de quipo funcionan sin operadores humanos.

Estado Actual: Definido

Basándose en las respuestas del formulario de evaluación de procesos de COBIT, y la aplicación de la fórmula para determinar el nivel de madurez, la DTIC se encuentra en un estado 3.7 de nivel de madurez el cual estable:

Se entiende y acepta a lo largo de toda la DTIC, la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la dirección. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo solo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas del centro de datos mantienen un perfil bajo y no son reconocibles de manera fácil.

VII. DISEÑO METODOLOGICO

Para la ejecución de esta auditoria se utilizaron diversas técnicas, para la recopilación de información necesaria para el desarrollo de la misma y posteriormente el procesamiento de esta información brindó los resultados para poder elaborar el informe final de la auditoria, por lo tanto, la realización de esta auditoria es de carácter cuantitativo.

Entre las técnicas están:

-**Análisis de la situación:** En esta fase se realizó la recopilación para el análisis de la información de la DTIC. Se solicitaron documentos para obtener conocimiento de la operatividad y manejo del área.

-**Entrevistas:** Dirigida al director de la DTIC y a responsables de unidad tanto de servidores, como del área de Infraestructura de Redes y Soporte Técnico. Se utilizó un formulario de evaluación de procesos de COBIT en el cual utiliza preguntas cerradas con el objetivo de recopilar las respuestas de los entrevistados dentro de un marco limitado de opciones. Las preguntas cerradas son la base de todas las técnicas de análisis estadístico aplicadas en cuestionarios y encuestas. Ver anexo 1.

-**Cuestionarios:** Método por el cual se busca obtener más información precisa de la que no se obtuvo de las entrevistas. Este cuestionario está basado en la normativa ISO 27002:2005 SEGURIDAD FISICA Y DEL ENTORNO.

- **Lista de cotejo** (**Observaciones):** En esta fase se procedió a observar las instalaciones, sistemas, cumplimiento de normas y procedimientos, no solo como espectador sino también como actor comprobando por sí mismo el funcionamiento de las instalaciones.

-**Hoja de procesamiento de datos (Microsoft Excel):** Herramienta ofimática para la clasificación de las respuestas

Las áreas a evaluar serán analizadas mediante La norma COBIT 4.1 la cual, contiene 34 procesos agrupados en 4 dominios: Planificación y Organización (PO), Adquisición e Implementación (AI), Entrega y Soporte (DS) y Monitoreo y Evaluación (ME). En cuanto a Auditoria de seguridad física los principales procesos para realizar este tipo de auditoría son la administración de instalaciones que corresponde al proceso 12 de Entrega y Soporte (DS 12), la cual contiene 5 objetivos de control: gestión del entorno físico, selección y diseño del centro de proceso de datos, medidas de seguridad física, acceso físico y protección contra factores ambientales, todos estos procesos se encuentran agrupados en el dominio de entrega y soporte (DS).

Se realizaron entrevistas a los principales responsables de unidad y también fueron verificadas sus respuestas a través de observaciones, listas de cotejos y cuestionarios, Para encontrar el resultado del modelo de madurez, se evaluó los resultados de los cuestionarios los cuales aplicamos los siguientes valores:

Bueno	Regular	Malo	No Aplicable
2	1	0	---

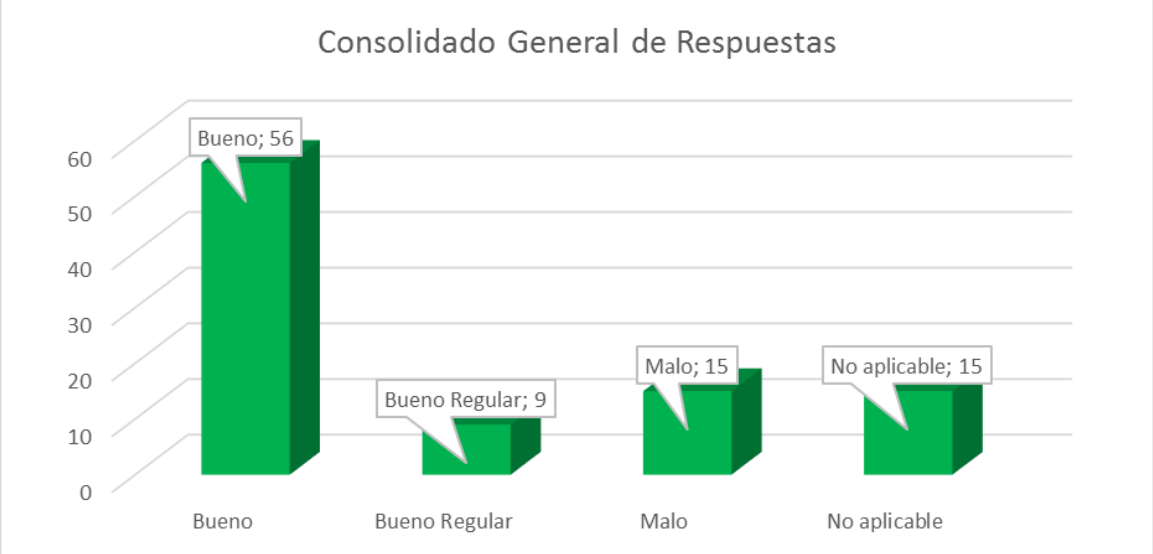

Fig. 7 Gráfica de repuestas al formulario de evaluación de procesos de COBIT.

Bueno: Para las respuestas que son afirmativas a las preguntas que si cumple con una buena gestión de TI establecida por la normativa COBIT 4.1.

Regular: Para las respuestas que no son exactas y tienen un nivel intermedio ni bueno, ni malo.

Malo: para las respuestas negativas que no cumple con una buena gestión de seguridad física en cuanto a la normativa COBIT establece.

No aplicable: a las preguntas que no existe ningún vínculo entre sí, es decir, por la inexistencia de aplicaciones o recursos de hardware.

En las preguntas cuyas respuestas es “No Aplicable” no se toman en cuenta para la evaluación. Se realizó un promedio de las respuestas de la entrevista y su resultado estará en el rango [0-2], también se realizó una equivalencia con el rango de [0-100] en el cual hacemos equivalencias de ambos valores máximos y decimos que 2 es a 100; ya teniendo esta equivalencia se puede establecer una regla de tres simples para así obtener la equivalencia en el rango de [0-100]:

2 → 100 ,X: es la equivalencia en la escala de [0-100]

P X , P: es el promedio de las respuestas de la entrevista en la escala [0-2]

$$X=\frac{P*100}{2} \qquad X=50P$$

Se realiza nuevamente la equivalencia, pero con el modelo de madurez que tiene valores en el rango [0-5], se igualan los valores máximos (5 es a 100) y se establece la regla de 3 simple para encontrar el nivel de madurez:

5 → 100 ,X: X=50P, es la equivalencia en la escala de [0-100]

Z X , Z: es el nivel de madurez en la escala de [0-5]

$$Z=\frac{X * 5}{100} = \frac{50P * 5}{100} = 2.5P$$

Z=2.5P , está es la fórmula para encontrar el nivel de madurez.

El modelo de madurez para la administración y el control de procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a si misma desde un nivel de no-existente (0) hasta un nivel optimizado (5). Este enfoque se deriva del modelo de madurez que el software engineering institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar donde se encuentran los problemas y como fijar prioridades para las mejoras. El propósito no es evaluar el nivel de adherencia a los objetivos de control.

VIII. CRONOGRAMA DE EJECUCION

PROGRAMA DE AUDITORIA			
INSTITUCION: DTIC-UNI		**FECHA:**	**HOJA N°**
FASE	ACTIVIDAD	SEMANAS ESTIMADAS	ENCARGADO
I	VISITA PRELIMINAR • Solicitud de Manuales y Documentaciones. • Elaboración de los cuestionarios. • Recopilación de la información organizacional: Infraestructura, recursos humanos, equipos.	**4**	**Jean Valencia**
II	DESARROLLO DE LA AUDITORIA • Aplicación del cuestionario al personal. • Entrevistas a líderes y usuarios más relevantes de la dirección. • Análisis de las claves de acceso, control, seguridad, confiabilidad y respaldos. • Evaluación de la estructura orgánica: departamentos, puestos, funciones, autoridad y responsabilidades. • Evaluación de los Recursos Humanos y de la infraestructura. • Evaluación de los sistemas: relevamiento de Hardware y Software, evaluación del diseño lógico y del desarrollo de los sistemas. • Evaluación del Data Center y de los Equipos de Cómputos: seguridad de los datos, control de operación, seguridad física y procedimientos de respaldo.	**12**	**Jean Valencia**
III	REVISION Y PRE-INFORME • Revisión de los papeles de trabajo. • Elaboración del Borrador.	**2**	**Jean Valencia**
IV	INFORME • Elaboración y presentación del Informe.	**2**	**Jean Valencia**

IX. OBSERVACIONES Y RECOMENDACIONES DETALLADAS

Plan de Mantenimiento de Hardware y Software

Hallazgo: La DTIC cuenta con un plan de mantenimiento de PC´s, equipos de redes y servidores, sin embargo, solo se realiza a 1 vez durante el año por tener poco personal, existen dos tipos de mantenimientos: mantenimiento preventivo y mantenimiento correctivo.

Se recomienda la creación formal de un plan de mantenimiento a ejecutarse dos veces al año y establecer los procedimientos de las tareas a realizar. Planes y procedimientos que deberán ser dados a conocer a todos los empleados del área acerca del correcto uso de los equipos informáticos para optimizar los servicios de mantenimiento, además se recomienda llevar un registro detallado de las actividades que se realizan en cada tarea y se ejecuten en tiempo y forma de acuerdo al plan.

Ejecutar un plan de contingencia adecuado

En general, desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa.

En la DTIC se cuenta con un plan de contingencia la cual establece la reactivación del antiguo centro de datos en caso de que el centro de datos principal quede fuera de servicio ya sea por desastre natural o por daños y robos causados por el hombre.

También se tiene previsto la ejecución de una réplica del centro de datos la cual estaría ubicada en la sede regional norte Recinto Universitario Augusto C. Sandino con el objetivo de mantener siempre en funcionamiento los servidores sin importar las condiciones en que se encuentre el nodo principal en la UNI-RUBS.

La probabilidad de que ocurra un desastre es muy baja, aunque, si se diera, el impacto podría ser tan grande que resultaría fatal para la DTIC. Se necesitan

medios para afrontarlo. Estos medios quedan definidos en el plan de recuperación de desastres que, junto con el centro alternativo de procesos de datos, constituye el plan de contingencia que coordina las necesidades y las operaciones de recuperación del mismo.

El plan de contingencia inexcusablemente debe:

- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas.

- Establecer un periodo crítico de recuperación en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.

- Realizar un análisis de aplicaciones críticas por el que se establecerán las prioridades de proceso.

- Determinar las prioridades de proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.

- Establecer objetivos de recuperación que determinen el periodo de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en que el centro alternativo puede procesar las aplicaciones críticas.

- Designar, entre los distintos tipos existentes, un centro alternativo de proceso de datos.

- Asegurar la capacidad de las comunicaciones y los servicios de Back-up.

En base al formulario de evaluación de procesos, se recomienda poder llevar a cabo la ejecución de las siguientes recomendaciones para logar ver resultados positivos de seguridad física en el Centro de Datos de la UNI según la metodología COBIT 4.1 se recomienda:

- ✓ Elaborar una lista de procedimientos por escrito para la ejecución de sus actividades dirigidos al personal de limpieza, mantenimiento y vigilancia.

- ✓ Asegurar la carcasa del servidor de archivos a fin de evitar cualquier retiro de dispositivos electrónicos.

- ✓ Situar el centro de datos en un piso intermedio (ni último piso, ni planta baja, preferible nivel intermedio).

- ✓ Tener una bóveda externa con adecuadas medidas de seguridad física que incluyen protección contra fuego, contra robos y con controles de temperatura y humedad para el almacenamiento de copias de seguridad.

- ✓ Contar un dispositivo cortafuego que impidan la propagación a través de los ductos.

- ✓ Realizar estudios de riesgos de incendio, considerando los aspectos de protección y prevención con un seguimiento de recomendaciones prescritas.

- ✓ Los cables empotrados en cañerías tengan un sistema de resistencia al fuego.

- ✓ Implementar detectores de agua debajo de pisos sobre elevados y cerca de los drenajes del piso que activen señal audible.

- ✓ El medio de control de acceso físico actúe de manera automática en caso de evacuación de personas en caso de desastre.

- ✓ Contar con un dispositivo alternativo para evacuar al personal de la sala de operaciones en caso de desastre que inhabilite los sistemas normales de ingreso y egreso.

- ✓ Evaluar el equipamiento de oficina del centro de datos su resistencia al fuego.

- ✓ La adquisición de muebles ignífugos donde guardar material sensible.

- ✓ Probar semestralmente el grupo electrógeno a fin de determinar el funcionamiento de las instalaciones durante el tiempo promedio de duración de los apagones.

X. CONCLUSIONES

Se ha culminado de manera satisfactoria el Plan de Auditoria de Sistemas de Información de la Seguridad Física en la DTIC utilizando la normativa COBIT 4.1, principalmente se ha evaluado las condiciones de seguridad existentes en el nuevo Centro de Datos de la UNI pudiendo constatar los procedimientos y controles que se utilizan actualmente para asegurar los equipos y el personal.

Sin embargo, según COBIT se necesitan adoptar procesos tales como: Definir la arquitectura de la Información en la cual se debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información, esto incluye el desarrollo de un diccionario de datos de la división, el esquema de clasificación de datos y los niveles de seguridad con el fin de mejorar la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable, segura y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias de la división.

Además de definir la arquitectura de la información, la División requiere de procesos como: Evaluar y Administrar los Riesgos de TI el cual sirve para dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la DTIC, causado por algún evento no planeado se debe identificar, analizar y evaluar.

También apoyarse del proceso: adquirir y mantener infraestructura tecnológica, que cuenta con procesos para adquirir, implementar y actualizar la infraestructura tecnológica, pero esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convencidas y la disposición de ambiente de desarrollo y pruebas.

XI. GLOSARIO DE TERMINOS

Auditoría: Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. Conjunto de métodos y técnicas con los que se preocupa identificar y evaluar algo.

Auditoría Informática: Evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoria, incluyendo el uso de software.

Aplicaciones: Programa preparado para una utilización específica, como el pago de nóminas, formación de un banco de términos léxicos, etc.

Fiduciarios: Persona que administra el dinero o los bienes de otras personas.

Pragmática: Relativo a la práctica o la realización de las acciones y no la teoría. Pragmático es un término de origen griego "pragmatikus" y latín "pragmaticu", que significa ser “práctico”.

Seguridad Física: Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Seguridad Lógica: Aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Servidor: En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Switch: Un switch o conmutador es un dispositivo de interconexión de redes informáticas. En computación y en informática de redes, un switch es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI u Open Systems Interconnection.

TI: Tecnología de información. Conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizado y utilizado en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad.

TIC´s: Tecnologías de la Información y la Comunicación, son el conjunto de tecnologías desarrolladas para gestionar información.

COBIT (Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. **COBIT** se utiliza para implementar el gobierno de IT y mejorar los controles de IT.

XII. BIBLIOGRAFÍA

- Piattini, M. y Navarro, E. *Auditoria Informática: un enfoque Práctico* 2ª. Edición; RA-MA Editorial; Madrid, España; 2001.

- Narváez, C. y Sevilla, H. (2012), Auditoria Informática Física y Lógica a la Empresa Almacenes Americanos S.A, Managua. Recuperado el 1 de marzo de 2017, de http://repositorio.uca.edu.ni/556/1/UCANI3501.PDF

- Rojas, I. (2013) Auditoría de Sistemas de Información, Córdoba. Recuperado el 20 de abril de 2017, de http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml

- ISACA.org (2007); COBIT 4.1 Estados Unidos de América. IT Governance Institute, http://www.isaca.org/cobit/pages/default.aspx

XIII. ANEXOS

ANEXO 1

Ejemplo de Cuestionario Meycor COBIT

Formulario de Evaluación de Procesos

Responsable: ADMIN

29 - Gestión del entorno físico (DS12)

Dominio: Entrega y Soporte

1)

1.1) ¿Se definen y seleccionan los emplazamientos físicos para el equipamiento de TI a fin de apoyar la estrategia tecnológica vinculada con la estrategia de negocio?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

1.2) ¿La selección y el diseño de la distribución del emplazamiento toman en cuenta los riesgos asociados con desastres naturales y causados por el hombre, al tiempo que consideran las leyes y reglamentaciones relevantes, como ser regulaciones de salud y seguridad laboral?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

2)

2.1) ¿Se definen e implementan medidas de seguridad física en línea con los requerimientos de negocio?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

2.2) ¿Estas medidas incluyen, entre otras, la distribución del perímetro de seguridad, de las zonas seguras, del emplazamiento del equipamiento crítico, y de las áreas de recepción y envío?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

2.3) ¿Se mantiene un perfil bajo respecto a la existencia de operaciones críticas de TI?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.4) ¿Se establecen responsabilidades por el monitoreo y los procedimientos de informe y resolución de los incidentes de seguridad física?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.5) ¿El equipamiento fue situado en el lugar apropiado para reducir al mínimo el acceso innecesario en áreas de trabajo?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.6) ¿El servicio de tratamiento de la información está protegido contra desastres naturales y generados por el hombre?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.7) ¿Existe alguna amenaza potencial proveniente de locales y áreas vecinas?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.8) ¿Existe una política con respecto al comer, beber y fumar en proximidad de los servicios de tratamiento de la información?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.9) ¿Fueron adoptados controles para reducir al mínimo el riesgo de amenazas potenciales tales como hurto, fuego, explosivos, humo, agua, polvo, vibraciones, agentes químicos, interferencias en el suministro eléctrico, radiación electromagnética e inundación?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.10) ¿Fueron aislados los artículos que requieren protección especial para reducir el nivel general de protección requerida?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.11) ¿Las áreas de tratamiento de la información y de entrega, están aisladas entre sí para evitar algún acceso no autorizado?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.12) ¿Los cuartos que tienen el servicio de tratamiento de la información, pueden ser cerrados o tienen gabinetes con llave o cajas de seguridad?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.13) ¿Qué controles de ingreso existen para permitir solamente al personal autorizado entrar en distintas áreas dentro de la organización?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.14) ¿Qué dispositivos de seguridad perimetral se han puesto en práctica para proteger el servicio de tratamiento de la información? Algunos ejemplos de tal dispositivo de seguridad son puerta de entrada con control de tarjeta, paredes, recepción, etc.

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.15) ¿Se realizó una evaluación de riesgo para determinar la seguridad en

tales áreas?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.16) ¿Son supervisadas las condiciones ambientales que afectarían adversamente las instalaciones de tratamiento de la información?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.17) ¿Existen estudios especializados (de arquitectos o ingenieros) sobre peligros debido a factores estructurales que puedan afectar el edificio en el que se hallan los locales informáticos, con un seguimiento de las recomendaciones?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.18) ¿Tiene el edificio habilitación municipal y de bomberos vigente?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.19) ¿Se toman medidas inmediatas en caso de retiro de un empleado, para que devuelva las llaves o tarjetas magnéticas de acceso, las tarjetas de identificación (ID) y la contraseña autorizada, cuando el control de acceso es automático, y se notifica a los miembros del área el status del empleado separado a los efectos operativos que correspondan?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.20) ¿Se evalúa periódicamente las posibles rutas de ingreso físico al Centro de Cómputos a efectos de comprobar que se encuentra habilitada sólo una?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

2.21) ¿El personal de limpieza, mantenimiento y vigilancia está sometido a las mismas normas de acceso físico que el personal informático y se lo orienta sobre cómo hacer su tarea sin afectar los equipos, todo ello mediante una hoja de instrucciones escrita?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.22) ¿Están los servidores y la documentación de la LAN ubicados en forma resguardada y razonablemente protegidos de accesos forzados, de acuerdo con directivas de la gerencia de informática, que es la responsable en la materia?

Clasificación: Redes en General

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.23) ¿Está trabada la carcasa del servidor de archivos o protegido de modo que no se retiren plaquetas, chips u otros dispositivos?

Clasificación: Microcomputadores

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.24) ¿Existe un registro de los poseedores responsables de las llaves del cuarto del servidor existente y el mismo se halla debidamente actualizado y funciona adecuadamente en la práctica?

Clasificación: Microcomputadores

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.25) ¿Se encuentra la sala de cómputos en un piso intermedio (ni último piso, ni planta baja ni subsuelo) del edificio, lejos de depósitos o almacenamiento de agua o líquido de cualquier naturaleza?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.26) ¿En caso de que la ubicación física del Centro de Cómputos se vaya a determinar y exista peligro de inundación, se prevé la posibilidad de colocar drenajes y darle un adecuado grado de inclinación al piso?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.27) ¿Existen previsiones para controlar en forma oportuna y eficaz situaciones de inundación por causas de cualquier naturaleza en áreas de concentración de equipos de computación?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.28) ¿La bóveda externa en la que se guarda las copias de respaldo cuenta con adecuadas medidas de seguridad física que incluyen protección contra fuego, contra robos y adecuados controles de temperatura y humedad?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.29) ¿Hay protección y vigilancia de las instalaciones de telecomunicaciones (borneras, unidades controladoras, módems, routers,

hubs, switches, etc.) disponiendo una ubicación segura para las mismas?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.30) ¿Se controla el acceso al lugar en donde se encuentra el AS/400?

Clasificación: AS/400

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.31) ¿El acceso al lugar en donde se encuentra el AS/400 por parte de personal que no es de la organización es debidamente registrado?

Clasificación: AS/400

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.32) ¿Las cintas y la documentación de respaldo se encuentran protegidas contra daños y robo?

Clasificación: AS/400

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.33) ¿Se definió que el conmutador de cerradura (keylock switch) de la unidad del sistema se ubique en la posición SECURE o AUTO?

Clasificación: AS/400

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.34) ¿Las llaves son removidas del panel del sistema y guardadas en lugares separados bajo extremas medidas de seguridad?

Clasificación: AS/400

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.35) ¿Los accesos a los locales informáticos son adecuados para una rápida llegada de bomberos, emergencia médica o policía, en caso de desastre?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.36) ¿En el caso de que la sensibilidad de la información de sus sistemas lo requiera, existe un sistema de control de acceso automático a los sectores destinados a instalaciones informáticas diferentes de la sala de operación o producción?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.37) ¿Hay un sistema automático de control de acceso a las salas de operación o producción?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

2.38) ¿Es correcto que, en caso de existir ventanas exteriores en áreas

sensibles del centro de cómputos, las mismas están protegidas contra acciones violentas o visualización desde el exterior?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

3)

3.1) ¿Se definen e implementan procedimientos para otorgar, limitar y denegar el acceso a las instalaciones, edificios y áreas de acuerdo a las necesidades del negocio, incluyendo emergencias?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

3.2) ¿Se justifica, autoriza, registra y monitorea el acceso a las instalaciones, edificios y áreas?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

3.3) ¿Esto se aplica a todas las personas que acceden a las instalaciones, incluyendo el personal habitual y temporal, los clientes, proveedores, visitantes y cualquier otro tercero?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

3.4) ¿Se lleva un registro histórico de los ingresos de visitantes, a los que se les entrega una tarjeta de identificación que deben llevar en lugar visible mientras permanecen en el Centro de Cómputos, reteniéndose su Cédula de Identidad mientras dura la visita?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

3.5) ¿Se realiza el ingreso al centro de cómputos por una única vía de acceso y se utilizan otras posibles vías exclusivamente para salida?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

3.6) ¿Se limita el acceso del personal al centro de cómputos fuera del horario normal, existiendo sensores de movimiento o cámaras de video a tales efectos?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

3.7) ¿Hay guardias apostados que verifiquen que el acceso se produzca de acuerdo con lo reglamentado?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

3.8) ¿Existe apoyo a la vigilancia por cámaras de video de grabación continua, para el ingreso a zonas sensibles?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

3.9) ¿Se halla limitado a personas autorizadas el acceso a locales que contienen hardware sensible?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

3.10) ¿Se ha concientizado debidamente al personal explicando la necesidad de implantar controles de acceso, uso de registros, control de visitas, etc.?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4)

4.1) ¿Se diseñan e implementan medidas de protección contra factores ambientales?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.2) ¿Se instala equipamiento y dispositivos especializados para monitorear y controlar el medio ambiente?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.3) ¿Existe, en el caso de contar con un sistema central de acondicionamiento de aire dispositivos cortafuegos que impidan que el fuego se propague de un lugar a otro a través de los ductos?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.4) ¿No existen problemas estructurales (mala impermeabilización, rotura de cañerías, humedad de cimientos, etc.) que eleven el nivel de la humedad relativa del local destinado a tareas informáticas?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.5) ¿No existen en un radio próximo a las instalaciones informáticas (mínimo tolerable 100 metros) depósitos de materiales inflamables o contaminantes, estacionamiento de coches, etc.?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.6) ¿Se han dispuesto las previsiones ambientales para garantizar que el servidor se mantenga dentro de las especificaciones técnicas del proveedor en materia de temperatura y humedad relativa?

Clasificación: Microcomputadores

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.7) ¿Están los disquetes y cintas protegidos de:

-daños por extremos de temperatura

-efectos magnéticos

-daños por agua?

Clasificación: Microcomputadores

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.8) ¿Existe un estudio específico de riesgo de incendio, considerando los aspectos protección y prevención, con un seguimiento de las recomendaciones prescritas?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.9) ¿Existen extinguidores manuales en la sala de cómputos? ¿Son los mismos adecuados para el tipo de incendio que pueden producirse (eléctrico, etc.)? ¿Conoce el personal su uso? ¿Se los prueba periódicamente?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.10) ¿Existen alarmas de incendio de accionamiento manual ubicadas estratégicamente en todo el centro y de fácil acceso para el personal, pero protegidas de modo de evitar su actuación accidental?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.11) ¿Existen sistemas de detección de humo por debajo y por encima de los paneles del cielorraso en todo el centro y por debajo del piso sobre elevado de la sala del computador, con ubicaciones marcadas para facilitar el acceso? ¿Producen los mismos una señal audible al activarse y avisan a un centro de vigilancia?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.12) ¿Existen sistemas automáticos de supresión de incendios cuando no hay atención humana permanente (¿24 horas? al día) que son probados periódicamente y evaluados en cuanto al daño que pueden producir si funcionan mal?

¿Existe un período de algunos segundos entre la alarma y la activación del supresor que permita abortar normalmente la operación en caso de error?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.13) ¿En el caso de existir sistemas de supresión de incendios automáticos o manuales basados en la emanación de gases adecuados a las necesidades, es correcto que los mismos no afectan la capa de ozono (FM 200, PROTRON, etc.)?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.14) ¿Existen inspecciones trianuales (o cuando se produce un cambio estructural importante) de Bomberos y se da cumplimiento a las recomendaciones recibidas?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.15) ¿Los pisos y paredes que rodean la sala del computador son de material incombustible con capacidad para resistir el fuego por lo menos una hora?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.16) ¿Los cables eléctricos empotrados y en cañerías tienen un adecuado sistema de resistencia al fuego?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.17) ¿Se minimiza la acumulación de material inflamable en el Centro de Cómputos, limitando en particular el suministro de papel a las necesidades semanales o quincenales?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.18) ¿Se ha evaluado el daño que puede ocasionar a las instalaciones el mal funcionamiento de los acondicionadores de aire o enfriadores de agua?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.19) ¿Hay estudios, controlados periódicamente por Ingenieros o Arquitectos especializados, sobre los peligros que pueden significar las cañerías de agua sobre las salas de los ordenadores y los materiales del entorno?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.20) ¿Se controla visualmente que no se produzca humedad en las paredes del Centro de Cómputos por fugas en las cañerías?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.21) ¿Existen detectores de agua debajo de pisos sobre elevados y cerca de los drenajes del piso que se activen mediante señal audible?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.22) ¿Existen detectores de agua ubicados encima de cielorrasos y debajo de las losas (si corresponde)?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.23) ¿En el caso de que se trate de una instalación pequeña y exista posibilidad de filtraciones de agua, se protegen las terminales e impresoras con cubiertas impermeables, cuando no se usan?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.24) ¿Se verifica que las ventanas o banderolas que tengan acceso al exterior queden cerradas cuando no hay personal de modo de evitar filtraciones de lluvia que puedan afectar a los equipos?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.25) En caso de existir cañerías de agua expuestas y en actividad dentro del Centro de Cómputos: ¿se verifica periódicamente el estado de las mismas y de sus conexiones por personal idóneo?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.26) En caso de existir cañerías de agua expuestas y en actividad dentro del Centro de Cómputos: ¿se ubican físicamente los equipos de modo que, en caso de ruptura de las mismas, el daño que pueda ocasionar sea minimizado?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.27) ¿La sala en donde se encuentra el AS/400 es a prueba de agua e incendio?

Clasificación: AS/400

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.28) ¿Se determina en que zonas del Centro de Cómputos debe prohibirse el fumar, señalizándolas mediante carteles y se vigila el cumplimiento estricto de esta medida?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

4.29) ¿Está el Centro de Computación adecuadamente aislado de vibraciones o ruidos externos intensos?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.30) ¿La iluminación de los locales informáticos y el acondicionamiento de aire son adecuados para el trabajo de las personas y cumplen con los requerimientos de higiene ambiental?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.31) ¿Los medios de control de acceso físico son coherentes con las eventuales necesidades de evacuación de personas en caso de desastre, desactivándose automáticamente en caso de alarma?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.32) ¿Existe un dispositivo alternativo para evacuar al personal de la sala de operaciones en caso de desastre que inhabilite los sistemas normales de ingreso y egreso?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.33) ¿Existen salidas de emergencia claramente marcadas y sin obstáculos desde el Centro de Cómputos hasta el exterior?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.34) ¿Al adquirir equipamiento de oficina para el Centro de Cómputos, se evalúa su resistencia al fuego?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.35) ¿Se tiene cerca del teléfono los números de incendio de Bomberos y/o se cuenta con un servicio de Bomberos interno de la empresa y se encuentra esta información en la documentación del Plan de Contingencia y Recuperación de Desastres.?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.36) ¿Conoce el personal de vigilancia la ubicación de los hidrantes existentes en la zona, saben si los mismos se hallan despejados y conocen la existencia de depósitos de agua cercanos que faciliten una intervención de Bomberos?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.37) ¿Existen dentro del Centro de Cómputos muebles ignífugos donde guardar, material sensible (respaldos aún no trasladados a la bóveda, etc.)?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

4.38) ¿Está prohibida en su instalación la ingestión de líquidos junto a los

equipos?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

5)

5.1) ¿Se gestionan las instalaciones, incluyendo el equipamiento de suministro de energía y comunicaciones, en línea con las leyes y reglamentaciones, los requerimientos técnicos y de negocio, las especificaciones de los proveedores y las pautas de salud y seguridad?

Clasificación: COBIT

() Bueno () Regular () Malo () No Aplicable

Comentario:
_____

5.2) ¿El equipamiento está protegido contra fallas eléctricas mediante fuentes de poder tales como múltiples alimentaciones, fuente de alimentación continua (UPS), generador de reserva, etc.?

Clasificación: ISO 17799

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

5.3) ¿Ha sido probado el grupo electrógeno dentro del último semestre y tiene una autonomía suficiente como para mantener el funcionamiento de las instalaciones durante el tiempo promedio de duración de los apagones?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

5.4) ¿Existe una o más UPS con capacidad adecuada que eviten las caídas del sistema en la conexión y la desconexión del grupo electrógeno?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

5.5) ¿Tiene previsto, el suministro de energía al Centro de Cómputos, recursos de alimentación de emergencia de energía (generador propio y UPS) para asegurar la continuidad de las operaciones durante un período razonable?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

5.6) ¿Existen previsiones que protejan la instalación informática y su cableado de sobrecargas imprevistas producto de tormentas eléctricas?

Clasificación: Orientación Específica

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

5.7) ¿Está la provisión de energía de la LAN controlada para garantizar que se mantenga dentro de las especificaciones técnicas del proveedor?

Clasificación: Redes en General

() Bueno () Regular () Malo () No Aplicable

Comentario:

_____

XIV. ANEXO 2

Cuestionario de Seguridad Física

¿Existe una política de seguridad física en la empresa y está actualizada?

SI____, NO____

¿Existen y se difunden los planes de contingencia/emergencia?

SI____, NO____

¿Existe un registro de todos los incidentes de seguridad y están clasificados según su gravedad?

SI____, NO____

¿Se han hecho análisis de riesgos de la seguridad física?

SI____, NO____

¿Se realizan simulacros/ejercicios en caso de emergencia?

SI____, NO____

¿La ubicación del Centro de Datos esta estudiada y documentada?

SI____, NO____

¿Existe un sistema de climatización adecuado?

Si____, NO____

¿Existe un sistema de control de acceso biométrico?

SI____, NO____

¿Todas las personas con acceso autorizado tienen una tarjeta de identificación y están controlados?

SI____, NO____

¿Existe un servicio de vigilantes de seguridad?

SI____, NO____

¿Existe un procedimiento especifico de control de acceso del personal de limpieza?

Si____, NO____

¿Existe un sistema automático de detección de incendios y está conectado a una central de alarmas?

SI____, NO____

¿Existe un indicador luminoso y sonoro fuera del Centro de Datos cuando el sistema contra incendios se dispara?

SI____, NO____

¿Está prohibido fumar en el Centro de Datos y se respeta esta prohibición?

SI____, NO____

¿Se ha hecho un estudio acerca de la posibilidad de inundaciones en la zona?

SI____, NO____

¿Existe un sistema de alimentación ininterrumpida?

SI____, NO____

XV. ANEXO 3

Evidencias gráficas de Auditoría

Fig.1 Sensor de temperatura.

Fig.2 Sistema Biometrico de control de huellas dactilares.

Fig.3 Sensor detector de humo.

Fig.4 Cable de fibra Optica expuesto.

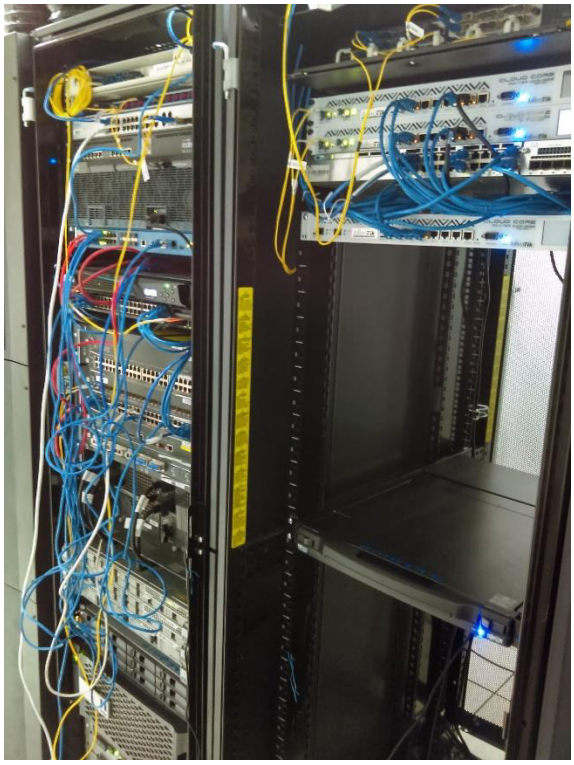

Fig.5 Servidor sin carcasa de seguridad expuesto.

Fig.6 UPS

Fig.7 Materiales de red en el suelo.

Fig.8 Cajas con materiales de red cerca del sistema de fluido contra fuego.

Fig.9 Sistema de refrigeracion de los servidores, tubos que extraen el aire caliente para ingresar aire frio.

Fig.10 Panel eléctrico.

Fig.11 Sistema de accionamiento manual contra incendios.

Fig.12 panel del sistema Novec

Fig.13 Tanque con el sistema de supresión de fuego Novec 1230.

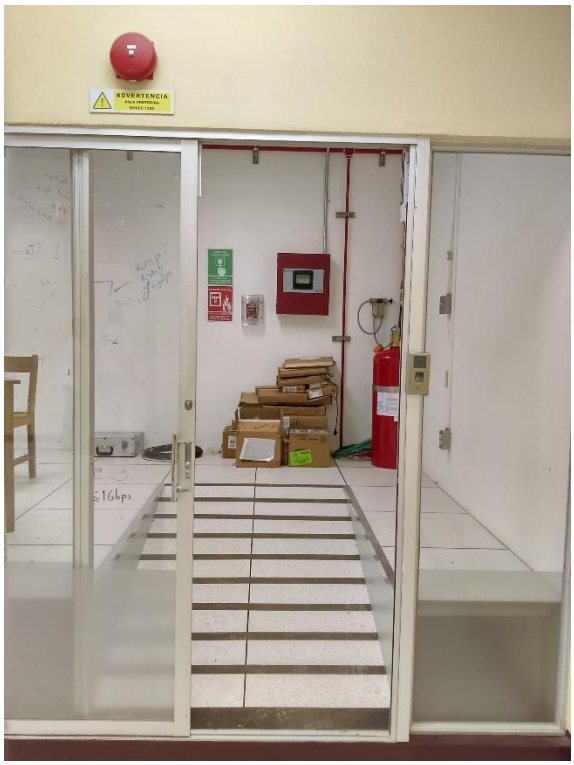

Fig.14 Entrada principal.

Fig.15 Alarma visual de Incendio.

Fig.16 Alarma sonora de incendio.

Fig.17 Antena WIFI dentro del Centro de Datos.

XVI. ANEXO 4

Informe de Auditoria

UNIVERSIDAD NACIONAL DE INGENIERÍA

DIVISIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN DTIC

INFORME:

AUDITORIA DE SISTEMAS DE INFORMACIÓN DE LA SEGURIDAD FÍSICA

Managua, Nicaragua

octubre de 2018

OBJETIVOS

Objetivo General

Presentar los resultados obtenidos durante el proceso de Auditoría de Sistemas de Información de la Seguridad Física aplicado a la División de Tecnologías de la Información y Comunicación DTIC

Objetivos Específicos

- Evaluar la situación actual de la DTIC en cuanto a seguridad física basado en la normativa COBIT 4.1.

- Identificar vulnerabilidades de seguridad física en los recursos, (tecnología, instalaciones, personal, comunicaciones de redes).

- Presentar informe de hallazgos y recomendaciones obtenidos de la ejecución del plan de auditoria.

- Conocer y evaluar la situación actual de la DTIC para la toma de decisiones.

ANTECEDENTES GENERALES

La División de Tecnologías de la Información y Comunicación DTIC, carece de antecedentes previos de Auditoria de Sistemas de Información de la Seguridad Física, así como también de documentación similar a una buena gestión de la seguridad física, su gestión consiste en la utilización de un sistema de mesa de ayuda (helpdesk), donde registran todas las incidencias del área de Infraestructura de Redes y Soporte Técnico, como también, del área de Administración de Servidores para realizar un seguimiento y control de las incidencias atendidas a los usuarios de la UNI, gestión que no contempla la seguridad física de la división, es por ello que nace esta propuesta de Auditoria de Sistemas de Información de la Seguridad Física como parte de la innovación en cuanto al tema y marcar un antecedente del mismo, además de ser un tema de interés tecnológico que contribuirá a la gestión de buenas prácticas de seguridad física en la DTIC y en la cual aplicaré mis conocimientos adquiridos durante los años de estudio en la carrera de Ingeniería en Computación.

El Centro de Datos de la UNI ubicado desde un inicio en el edificio de la Facultad de Electrotecnia y Computación (FEC), 2da planta, es administrado por la DTIC desde el año 2006 y nace con financiamiento de la cooperación internacional (Agencia Sueca para el desarrollo Internacional ASDI).

Actualmente, con la aprobación de un proyecto de nueva ubicación e instalación del Centro de Datos de la UNI se pretende modernizar los equipos de redes y su infraestructura para brindar un mejor servicio de ancho de banda de Internet a todas las áreas administrativas y académicas de la Universidad. Ubicado estratégicamente en el sótano del edificio Rigoberto López Pérez, se realizaron todos los estudios correspondientes en el año 2014, para ser aprobado por la dirección superior del consejo Universitario en el año 2015 solicitando la partida presupuestaria a través de un préstamo que realizo la Universidad en el año 2016, para finalmente implementarse en el mes de mayo de 2017 y ser administrado actualmente por el área Nic.ni la cual es un área de la Universidad Nacional de

Ingeniería (UNI) que además de administrar los dominios **NIC.NI** a nivel mundial, ofrece servicios de hosting, página web y otros, que son de mucha utilidad para los jóvenes universitarios, la sociedad y el país.

En las nuevas instalaciones del Centro de Datos de la UNI, es donde se aplicará el Plan de Auditoria de Sistemas de Información de la Seguridad Física utilizando la metodología COBIT 4.1 para determinar si estas instalaciones son las adecuadas en términos de seguridad física para una buena gestión de tecnologías de la información.

ALCANCE DE LA AUDITORIA

El plan de Auditoria de Sistemas de Información de la Seguridad Física desarrollado en la DTIC, está orientado a evaluar genéricamente el desempeño de las áreas que la componen y se apoya en la metodología de objetivos de control de COBIT 4.1, obteniendo de estos, los instrumentos necesarios para el desarrollo de dicho estudio. Conforme a los objetivos específicos de esta auditoria se realizó un trabajo de investigación en el cual se limita al resultado de la identificación y evaluación de la DTIC, la identificación y evaluación de los procesos que se utilizan, la aplicación de COBIT 4.1, el análisis de COBIT 4.1 y los resultados de la implementación.

Asimismo, se evaluaron las tres áreas principales de la DTIC como son la oficina de Infraestructura de Redes y Soporte Técnico, oficina de Sistemas de Información, oficina de Administración de Servidores y la más importante las instalaciones del nuevo Centro de Datos de la UNI.

Cabe mencionar, que esta auditoría de Sistemas de Información de la Seguridad Física fue realizada entre el periodo de octubre de 2017 a mayo de 2018, tiempo por el cual no se limitó ni restringió el acceso a la información por parte de la dirección de la DTIC.

Con los resultados de esta auditoría, se pretende guiar a la DTIC hacia mejor uso de las TIC´s en cuanto a la seguridad física, ayudar en la toma de decisiones, proteger los activos físicos y del personal, así como también, lograr la confidencialidad, integridad y disponibilidad de los Sistemas de Información y Comunicaciones mediante un informe de hallazgos y recomendaciones detalladas en este informe.

METODOLOGÍA

Para la ejecución de esta auditoria se utilizaron diversas técnicas, para la recopilación de información necesaria para el desarrollo de la misma y posteriormente el procesamiento de esta información brindó los resultados para poder elaborar el informe final de la auditoria, por lo tanto, la realización de esta auditoria es de carácter cuantitativo.

Entre las técnicas están:

-**Análisis de la situación:** En esta fase se realizó la recopilación para el análisis de la información de la DTIC. Se solicitaron documentos para obtener conocimiento de la operatividad y manejo del área.

-**Entrevistas:** Dirigida al director de la DTIC y a responsables de unidad tanto de servidores, como del área de Infraestructura de Redes y Soporte Técnico. Se utilizó un formulario de evaluación de procesos de COBIT en el cual utiliza preguntas cerradas con el objetivo de recopilar las respuestas de los entrevistados dentro de un marco limitado de opciones. Las preguntas cerradas son la base de todas las técnicas de análisis estadístico aplicadas en cuestionarios y encuestas. Ver anexo 1.

-**Cuestionarios:** Método por el cual se busca obtener más información precisa de la que no se obtuvo de las entrevistas. Este cuestionario está basado en la normativa ISO 27002:2005 SEGURIDAD FISICA Y DEL ENTORNO.

- **Lista de cotejo** (**Observaciones):** En esta fase se procedió a observar las instalaciones, sistemas, cumplimiento de normas y procedimientos, no solo como espectador sino también como actor comprobando por sí mismo el funcionamiento de las instalaciones.

-**Hoja de procesamiento de datos (Microsoft Excel):** Herramienta ofimática para la clasificación de las respuestas

Las áreas a evaluar serán analizadas mediante La norma COBIT 4.1 la cual, contiene 34 procesos agrupados en 4 dominios: Planificación y Organización (PO), Adquisición e Implementación (AI), Entrega y Soporte (DS) y Monitoreo y Evaluación (ME). En cuanto a Auditoria de seguridad física los principales procesos para realizar este tipo de auditoría son la administración de instalaciones que corresponde al proceso 12 de Entrega y Soporte (DS 12), la cual contiene 5 objetivos de control: gestión del entorno físico, selección y diseño del centro de proceso de datos, medidas de seguridad física, acceso físico y protección contra factores ambientales, todos estos procesos se encuentran agrupados en el dominio de entrega y soporte (DS).

Se realizaron entrevistas a los principales responsables de unidad y también fueron verificadas sus respuestas a través de observaciones, listas de cotejos y cuestionarios, Para encontrar el resultado del modelo de madurez, se evaluó los resultados de los cuestionarios los cuales aplicamos los siguientes valores:

Bueno	Regular	Malo	No Aplicable
2	1	0	---

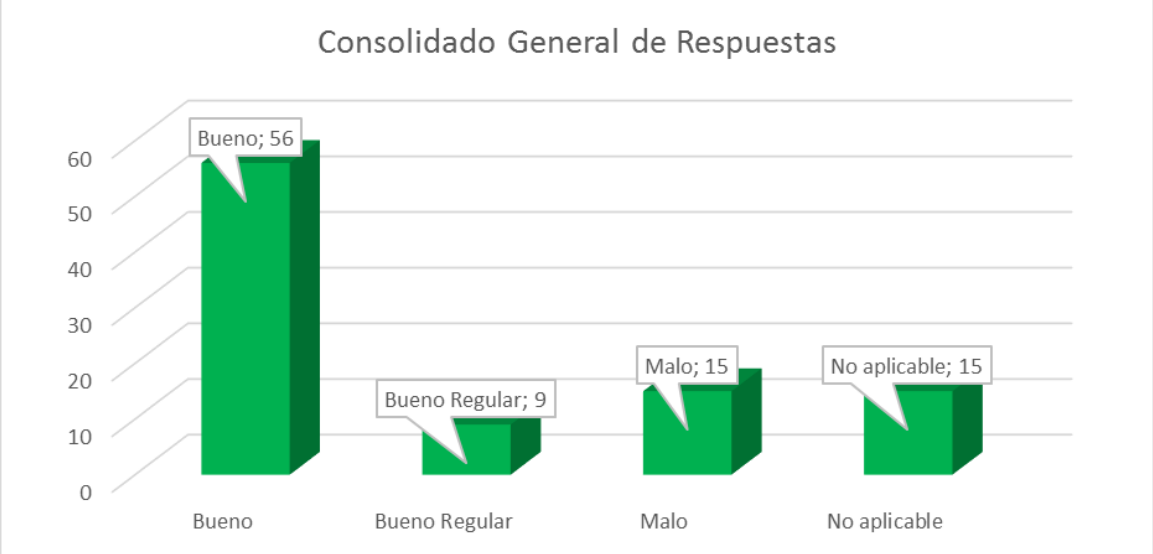

Fig. 7 Gráfica de repuestas al formulario de evaluación de procesos de COBIT.

Bueno: Para las respuestas que son afirmativas a las preguntas que si cumple con una buena gestión de TI establecida por la normativa COBIT 4.1.

Regular: Para las respuestas que no son exactas y tienen un nivel intermedio ni bueno, ni malo.

Malo: para las respuestas negativas que no cumple con una buena gestión de seguridad física en cuanto a la normativa COBIT establece.

No aplicable: a las preguntas que no existe ningún vínculo entre sí, es decir, por la inexistencia de aplicaciones o recursos de hardware.

En las preguntas cuyas respuestas es “No Aplicable” no se toman en cuenta para la evaluación. Se realizó un promedio de las respuestas de la entrevista y su resultado estará en el rango [0-2], también se realizó una equivalencia con el rango de [0-100] en el cual hacemos equivalencias de ambos valores máximos y decimos que 2 es a 100; ya teniendo esta equivalencia se puede establecer una regla de tres simples para así obtener la equivalencia en el rango de [0-100]:

2 → 100 ,X: es la equivalencia en la escala de [0-100]

P X , P: es el promedio de las respuestas de la entrevista en la escala [0-2]

$$X=\frac{P*100}{2} \qquad X=50P$$

Se realiza nuevamente la equivalencia, pero con el modelo de madurez que tiene valores en el rango [0-5], se igualan los valores máximos (5 es a 100) y se establece la regla de 3 simple para encontrar el nivel de madurez:

5 → 100 ,X: X=50P, es la equivalencia en la escala de [0-100]

Z X , Z: es el nivel de madurez en la escala de [0-5]

$$Z=\frac{X * 5}{100} = \frac{50P * 5}{100} = 2.5P$$

Z=2.5P , está es la fórmula para encontrar el nivel de madurez.

El modelo de madurez para la administración y el control de procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a si misma desde un nivel de no-existente (0) hasta un nivel optimizado (5). Este enfoque se deriva del modelo de madurez que el software engineering institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar donde se encuentran los problemas y como fijar prioridades para las mejoras. El propósito no es evaluar el nivel de adherencia a los objetivos de control.

OPINION GENERAL

El plan de Auditoria de Sistemas de Información de la Seguridad Física ejecutado en la División de Tecnologías de la Información y Comunicación DTIC, transciende sin lugar a dudas la importancia a los procedimientos de seguridad física que requiere la división, es evidente, que el estado actual de la división no está del todo ineficiente en cuanto a seguridad física de los equipos, sin embargo existen ciertas debilidades para garantizar la seguridad de dichos equipos tecnológicos y esto tiene que ver al aplicar medidas de prevención contra fenómenos naturales, que beneficiarían tanto al equipo informático como al personal, bastaría con aplicar las recomendaciones sugeridas en este informe para llenar esos vacíos que existen en cuanto a la seguridad física y así estar alertas ante desastres físicos o causados por el hombre en un futuro no muy lejano.

Por tanto, dentro del ámbito de la seguridad física, es sobradamente conocido el grave impacto que los desastres naturales tienen sobre las infraestructuras de todo tipo, de las que los sistemas informáticos forman parte, y de las que así mismo dependen para su adecuado funcionamiento.

En lo específico y con relación al objetivo central de esta auditoría, valoró positivamente aspectos elementales de funcionamiento, tales como:

- Existencia de un sistema (mesa de ayuda), para monitorear las incidencias atendidas a los usuarios de la Universidad.
- Identificación biométrica para acceso no autorizado al Centro de Datos.
- Medidas contra incendios.
- Medidas de respaldo de los Sistemas de Información.

No obstante, como menciono anteriormente, existen debilidades de alto riesgo asociadas a la seguridad del personal y seguridad de los equipos informáticos como: gabinetes de red expuestos, hubs y equipos inalámbricos al alcance de usuarios, equipos de red como switches, hubs, equipos inalámbricos sin protección contra altos voltajes.

OBSERVACIONES Y RECOMENDACIONES DETALLADAS

Plan de Mantenimiento de Hardware y Software

Hallazgo: La DTIC cuenta con un plan de mantenimiento de PC´s, equipos de redes y servidores, sin embargo, solo se realiza a 1 vez durante el año por tener poco personal, existen dos tipos de mantenimientos: mantenimiento preventivo y mantenimiento correctivo.

Se recomienda la creación formal de un plan de mantenimiento a ejecutarse dos veces al año y establecer los procedimientos de las tareas a realizar. Planes y procedimientos que deberán ser dados a conocer a todos los empleados del área acerca del correcto uso de los equipos informáticos para optimizar los servicios de mantenimiento, además se recomienda llevar un registro detallado de las actividades que se realizan en cada tarea y se ejecuten en tiempo y forma de acuerdo al plan.

Ejecutar un plan de contingencia adecuado

En general, desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa.

En la DTIC se cuenta con un plan de contingencia la cual establece la reactivación del antiguo centro de datos en caso de que el centro de datos principal quede fuera de servicio ya sea por desastre natural o por daños y robos causados por el hombre.

También se tiene previsto la ejecución de una réplica del centro de datos la cual estaría ubicada en la sede regional norte Recinto Universitario Augusto C. Sandino con el objetivo de mantener siempre en funcionamiento los servidores sin importar las condiciones en que se encuentre el nodo principal en la UNI-RUBS.

La probabilidad de que ocurra un desastre es muy baja, aunque, si se diera, el impacto podría ser tan grande que resultaría fatal para la DTIC. Se necesitan medios para afrontarlo. Estos medios quedan definidos en el plan de recuperación de desastres que, junto con el centro alternativo de procesos de datos, constituye el plan de contingencia que coordina las necesidades y las operaciones de recuperación del mismo.

El plan de contingencia inexcusablemente debe:

- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas.

- Establecer un periodo crítico de recuperación en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.

- Realizar un análisis de aplicaciones críticas por el que se establecerán las prioridades de proceso.

- Determinar las prioridades de proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.

- Establecer objetivos de recuperación que determinen el periodo de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en que el centro alternativo puede procesar las aplicaciones críticas.

- Designar, entre los distintos tipos existentes, un centro alternativo de proceso de datos.

- Asegurar la capacidad de las comunicaciones y los servicios de Back-up.

- Entre otras cosas, se recomienda poder llevar a cabo la ejecución de las siguientes recomendaciones para logar ver resultados positivos de seguridad física en el Centro de Datos de la UNI según la metodología COBIT 4.1:

- Se recomienda elaborar una lista de procedimientos por escrito para la ejecución de sus actividades dirigidos al personal de limpieza, mantenimiento y vigilancia.

- Se recomienda asegurar la carcasa del servidor de archivos a fin de evitar cualquier retiro de dispositivos electrónicos.
- Se recomienda situar el centro de datos en un piso intermedio (ni último piso, ni planta baja).

- Se recomienda tener una bóveda externa con adecuadas medidas de seguridad física que incluyen protección contra fuego, contra robos y adecuados controles de temperatura y humedad para el almacenamiento de copias de seguridad.

- Se recomienda contar un dispositivo cortafuego que impidan la propagación a través de los ductos.

- Se recomienda realizar estudios de riesgos de incendio, considerando los aspectos de protección y prevención con un seguimiento de recomendaciones prescritas.

- Se recomienda que los cables empotrados en cañerías tengan un adecuado sistema de resistencia al fuego.

- Se recomienda implementar detectores de agua debajo de pisos sobre elevados y cerca de los drenajes del piso que activen señal audible.

- Se recomienda que el medio de control de acceso físico actué de manera automática en caso de evacuación de personas en caso de desastre.

- Se recomienda contar con un dispositivo alternativo para evacuar al personal de la sala de operaciones en caso de desastre que inhabilite los sistemas normales de ingreso y egreso.

- Se recomienda evaluar el equipamiento de oficina del centro de datos su resistencia al fuego.

- Se recomienda la adquisición de muebles ignífugos donde guardar material sensible.

- Se recomienda probar semestralmente el grupo electrógeno a fin de determinar el funcionamiento de las instalaciones durante el tiempo promedio de duración de los apagones.

CONCLUSIONES

Se ha culminado de manera satisfactoria el Plan de Auditoria de Sistemas de Información de la Seguridad Física en la DTIC utilizando la normativa COBIT 4.1, principalmente se ha evaluado las condiciones de seguridad existentes en el nuevo Centro de Datos de la UNI pudiendo constatar los procedimientos y controles que se utilizan actualmente para asegurar los equipos y el personal.

Sin embargo, según COBIT se necesitan adoptar procesos tales como: Definir la Arquitectura de la Información en la cual se debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información, esto incluye el desarrollo de un diccionario de datos de la división, el esquema de clasificación de datos y los niveles de seguridad con el fin de mejorar la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable, segura y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias de la división.

Además de definir la Arquitectura de la Información, la División requiere de procesos como: Evaluar y Administrar los Riesgos de TI el cual sirve para dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la DTIC, causado por algún evento no planeado se debe identificar, analizar y evaluar.

También apoyarse del proceso: Adquirir y Mantener Infraestructura Tecnológica, que cuenta con procesos para adquirir, implementar y actualizar la infraestructura tecnológica, pero esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convencidas y la disposición de ambiente de desarrollo y pruebas.

CARTA DE AUTORIZACION Y EVIDENCIAS GRAFICAS

UNIVERSIDAD NACIONAL DE INGENIERIA
DIVISION DE TENCOLOGIAS DE LA INFORMACION Y COMUNICACION
Managua, Nicaragua

Viernes, 04 de agosto 2017

Jean Fracois Valencia
Técnico Informático DTIC
Universidad Nacional de Ingeniería

Sus manos.

Estimado colaborador Valencia antes de todo reciba un cordial saludo, y éxitos en el desempeño de sus funciones.

En respuesta a su carta fechada 03 de agosto 2017, donde solicita espacio investigativo en la DTIC, para realizar un plan de **Auditoria Informática de la Seguridad Física**, como tesis monográfica para optar a título de ingeniero en un periodo estimado de seis meses a partir del 15 de agosto del presente año, tomando en cuenta que el resultado de ese estudio sirva a la DTIC como retroalimentación positiva en aras de mejoras de los servicios TIC´S, le consedo el espacio investigativo a su solicitud.

Atentamente.

MGP. Sixto Chavarría Carrión
Director DTIC

Archivo

Fig.1 Carta de la dirección con la aprobación de la auditoria.

Fig.2 Material de fácil combustión en el cuarto de servidores.

Fig.3 Materiales de red en el piso.

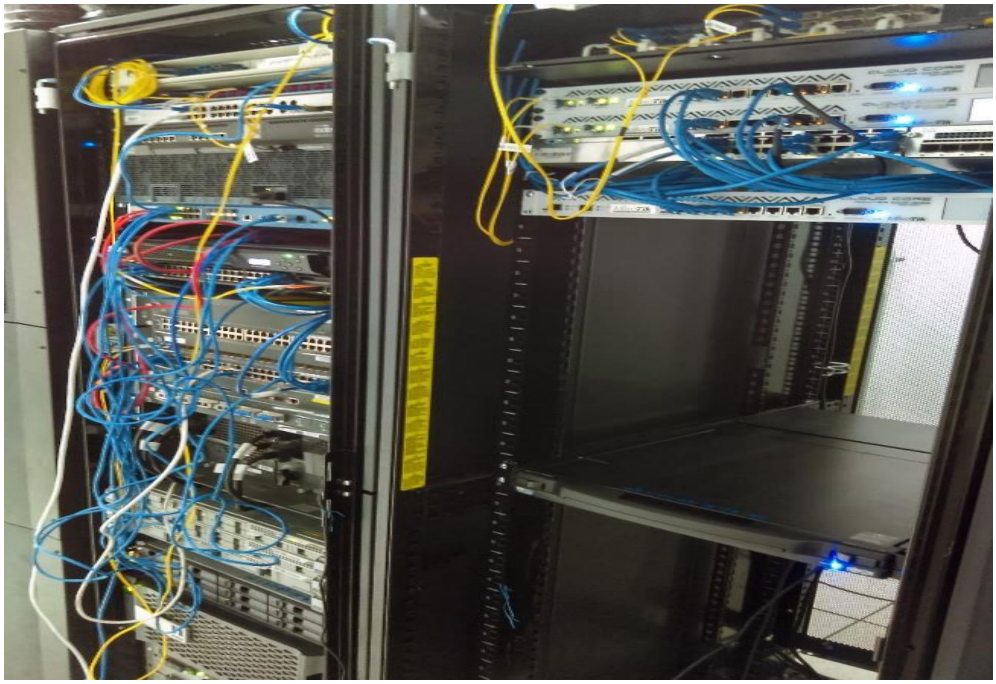

Fig.4 Servidor sin carcasa de seguridad.

Fig.5 Cable de fibra Optica no empotrado y expuesto a daños.

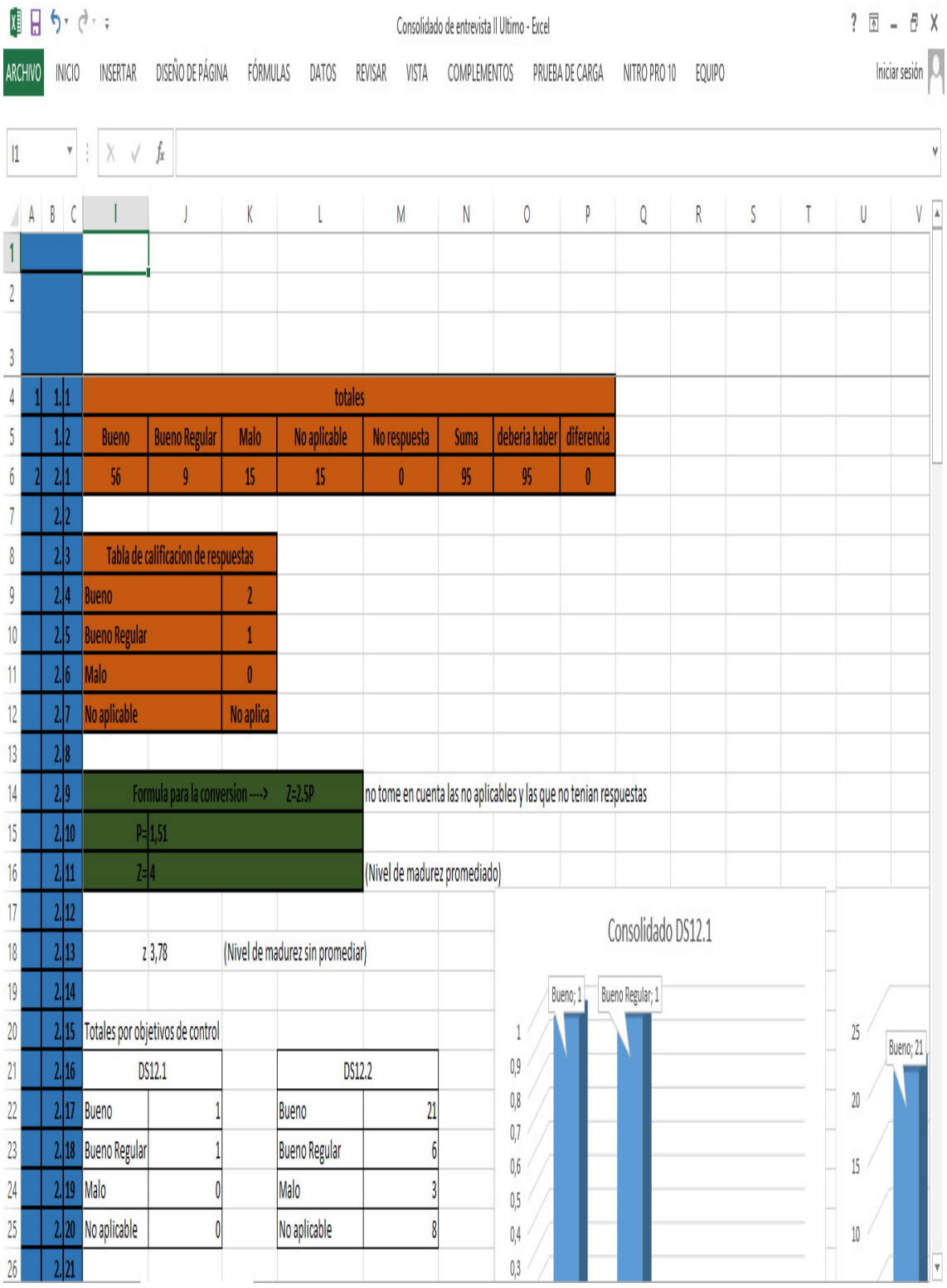

Fig. 6 Herramienta Ofimatica para el procesamiento de las respuestas al formulario de evaluacion de procesos de COBIT 4.1